Hot Topic Forum: Cloud Computing

onsored by the DAU Alumni Association

30 March 2011

Chris Knepper

Partner, Cloud Consulting Practice
CSC

Mike Dorohovich

Army Land Division
CSC

The Conversation

- Why are we here? Because Cloud Computing is Hot!
- A very brief overview of “Cloud Computing”
- Federal Government and Cloud Computing
- Cloud Computing Strategy
- Cloud Computing Security Considerations

Why are we here? Because Cloud Computing is Hot!

Gartner released a study which highlighted the top 10 strategic technologies for 2011.

At the top of the list is Cloud Computing!

Cloud Computing. Cloud computing services exist along a spectrum from open public to closed private. The next three years will see the delivery of a range of cloud service approaches that fall between these two extremes. Vendors will offer **packaged private cloud implementations** that deliver the vendor's public cloud service technologies (software and/or hardware) and methodologies (i.e., best practices to build and run the service) in a form that can be implemented inside the consumer's enterprise. Many will also offer **management services** to remotely manage the cloud service implementation. Gartner expects large enterprises to have a dynamic sourcing team in place by 2012 that is responsible for ongoing cloud-sourcing decisions and management.

Source: http://www.gartner.com/it/page.jsp?id=1454221

An Evolution of Cloud Computing

A little older than we thought …

Google Search as a Service
eBay Auction as a Service
Facebook Social Networking as a Service
Twitter Micro-blogging as a Service
Wikipedia Knowledge as a Service
Symplified Identity and Authentication as a Service
… Lots of stuff "… as a Service"

hotmail
First real cloud computing service

twitter
myspace.com
a place for friends
Wikipedia
YouTube
facebook
Blogger
LinkedIn
ebay
Google
Second Life

… Software as a service for enterprise use

Amazon has excess capacity to meet seasonal buying needs

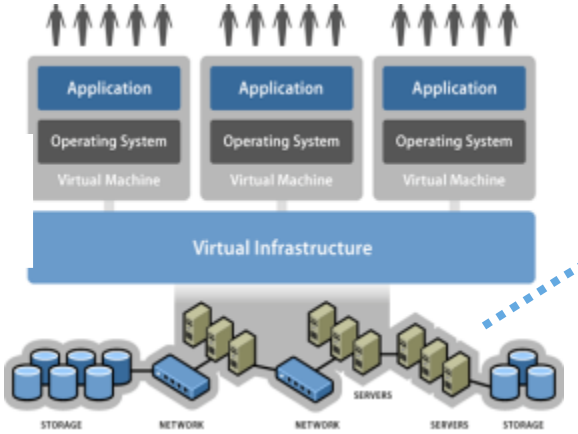
Amazon starts a business to rent idle infrastructure

amazon web services™

First successful business offering Infrastructure-as-a-Service for enterprise use

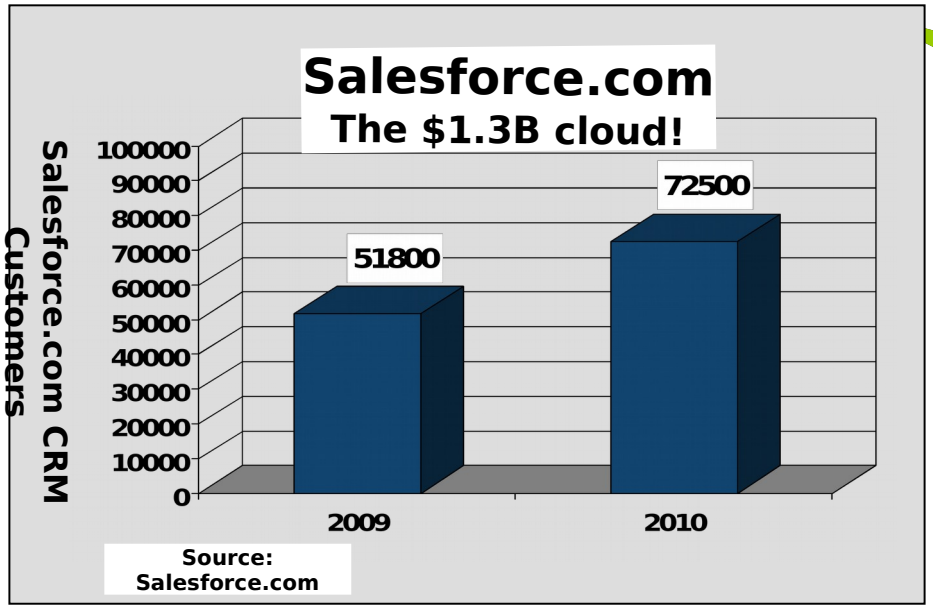
Cloud Computing

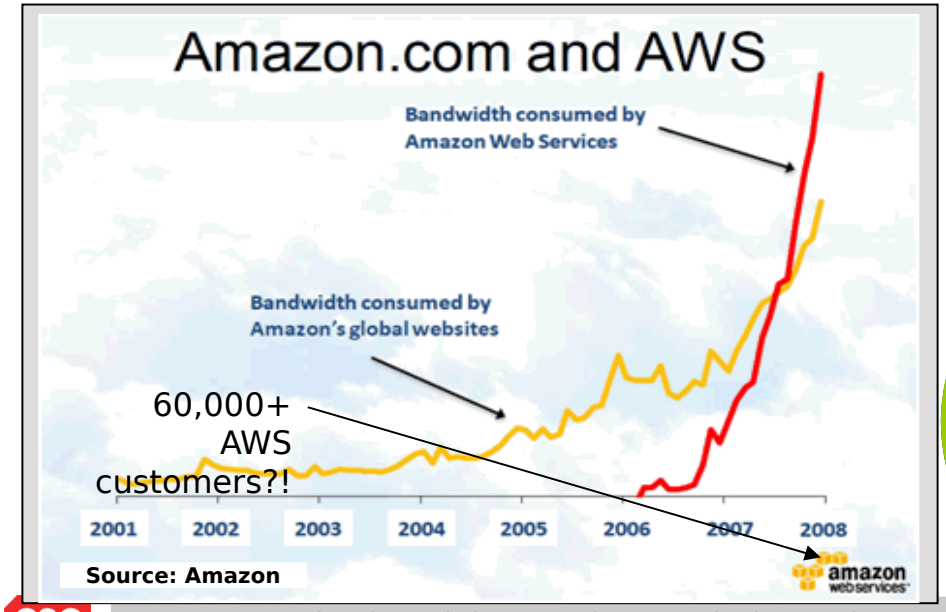
Wide-scale implementation of virtualisation within all major enterprise IT environments

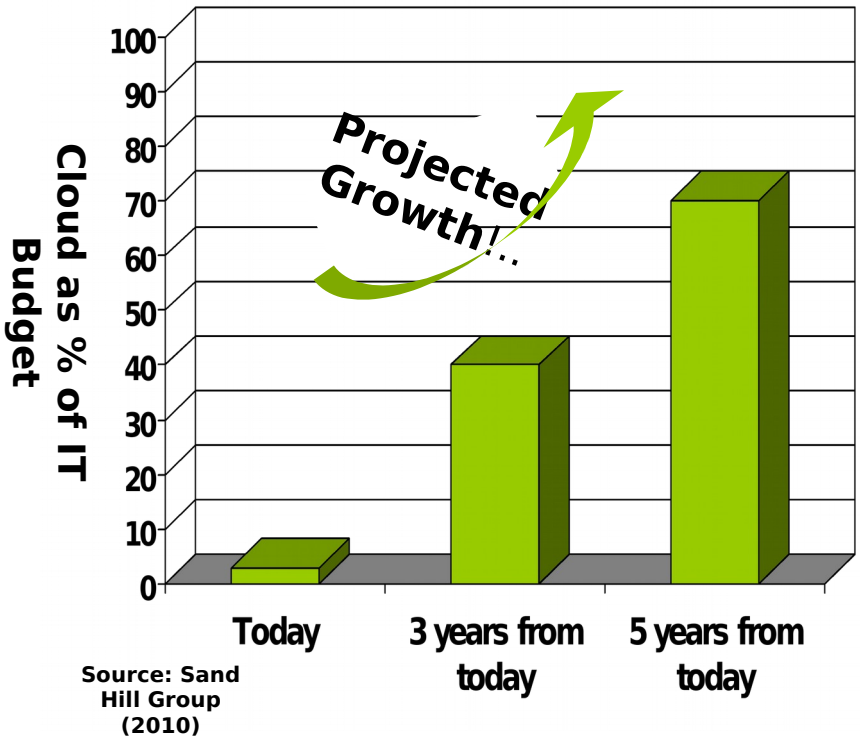


Virtualisation enables many elements of Cloud Computing

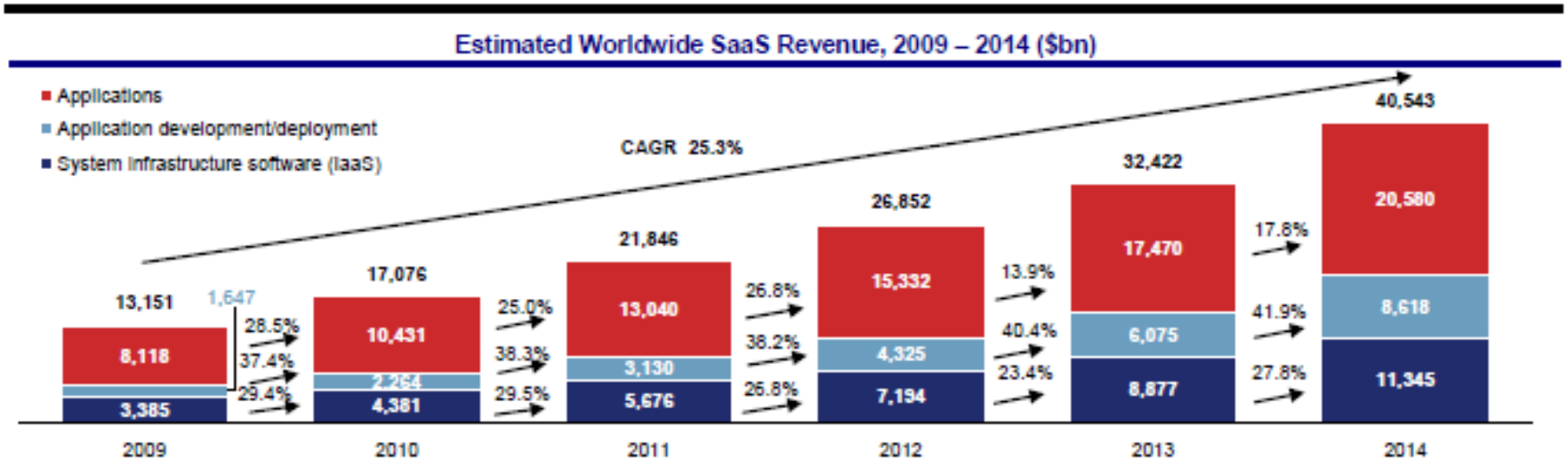
Some (Most?) of My Best Friends Use It!

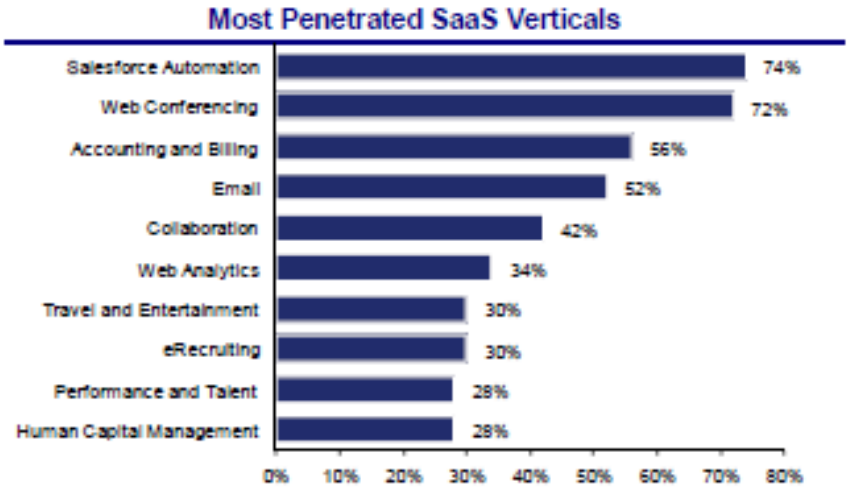






Cloud Computing Rapid Adoption





Source: IDC, May2010; Goldman Sachs Research

The Conversation

- ✓ Why are we here? Because Cloud Computing is Hot!
- ➢ A very brief overview of “Cloud Computing”
- Federal Government and Cloud Computing
- Cloud Computing Strategy
- Cloud Computing Security Considerations

Cloud Computing is Characterized by Four Key Attributes

Definition	Key Attributes	Customer Needs
A style of computing where massively scalable, IT-enabled capabilities are provided "as a service" across the Internet to multiple external customers	*Acquisition Model* **Service** *Business Model* **Pay for usage** *Access Model* **Internet** *Technical Model* **Scalable, elastic, shareable**	"All that matters is results — I don't care how it is done" "I don't want to own assets — I want to pay for elastic usage, like a utility" "I want accessibility from anywhere from any device" "It's about economies of scale, with effective and dynamic sharing"

Multiple Models of Cloud Computing

Cloud computing is a model for enabling **on-demand network access** to a **shared pool of configurable computing resources** that can be **rapidly provisioned and released** with **minimal management effort** or service provider interaction OR simply
"IT you run over the Internet instead of installing hardware and software yourself"

Characteristics

On demand self service

Pay as you use

Rapid elasticity (expand/contract)

Multi tenancy (shared pool)

Broad network

Service Models

Deployment Models

- Public Cloud
- Community Cloud
- Hybrid Cloud
- Private Cloud

Cloud Computing Service Models

- *Cloud Software as a Service (SaaS).*
  - The capability provided to the consumer is to use **the provider's applications** running on a **cloud infrastructure** and accessible from various client devices through a thin client interface such as a Web browser (e.g., web-based email).
- *Cloud Platform as a Service (PaaS).*
  - The capability provided to the consumer is **to deploy onto the cloud** infrastructure **consumer-created applications** using programming languages and tools supported by the provider (e.g., java, python, .Net).
- *Cloud Infrastructure as a Service (IaaS)*
  - The capability provided to the consumer is **to provision processing, storage, networks**, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Cloud Computing Deployment Models

- *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g.,

Defining "Cloud Computing" …

- NIST provides a formal definition…

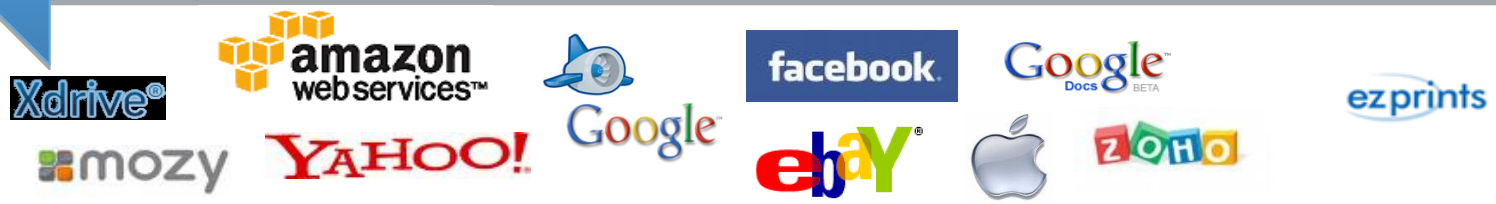
"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of **five** essential characteristics, **three** service models, and **four** deployment models."

Authors: Peter Mell and Tim Grance, Version 15, 10-7-09

Reference: NIST.gov

Many Cloud Computing Offerings

System Infrastructure | **Application Infrastructure** | **Application and Information** | **Process**



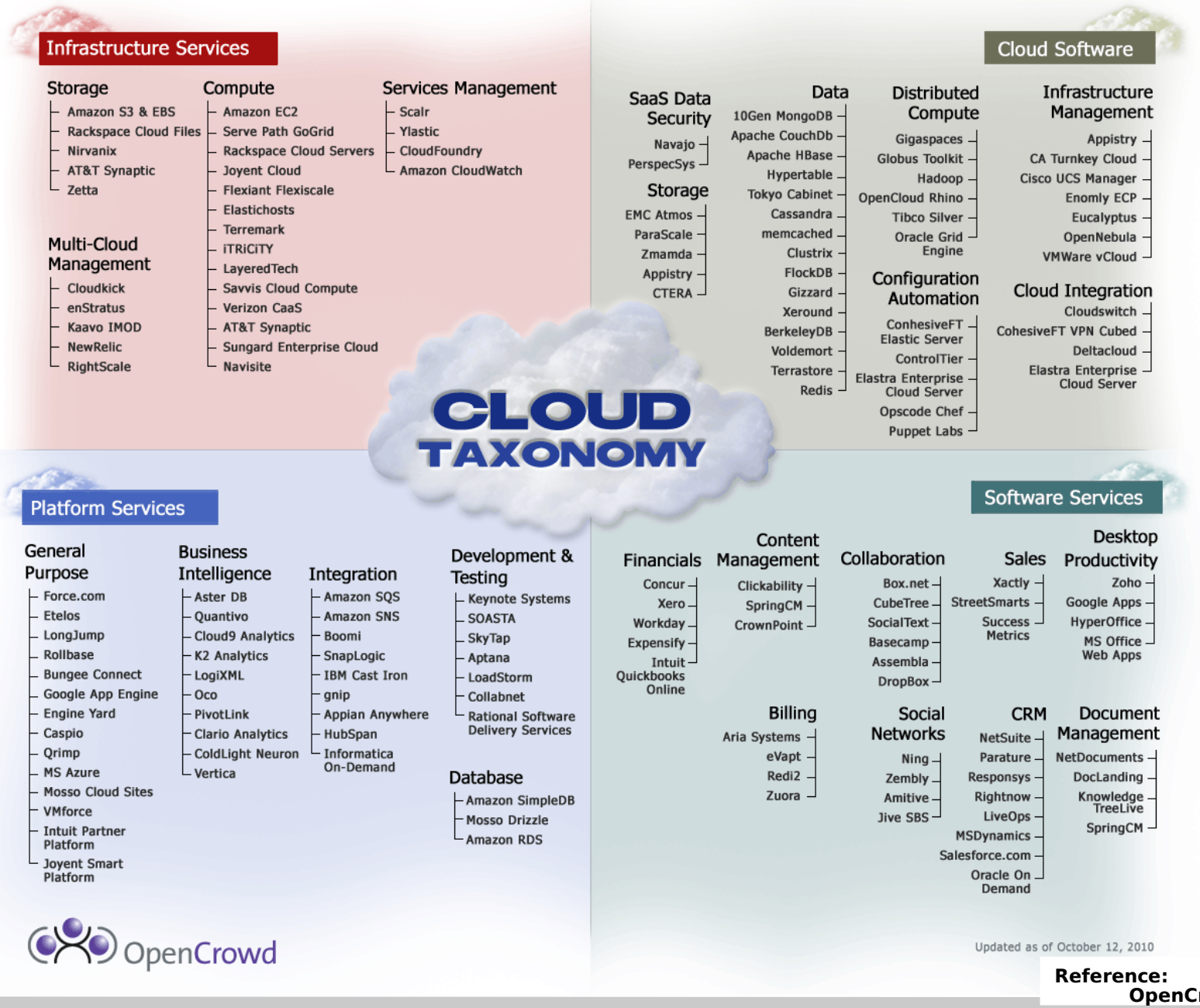
Business/Enterprise Influenced

Consumer/Web Influenced

* A sample list only. There are many more players.

An evolving Public Sector Cloud ecosystem

Clouds are Getting Crowded



Reference: OpenCrowd.com

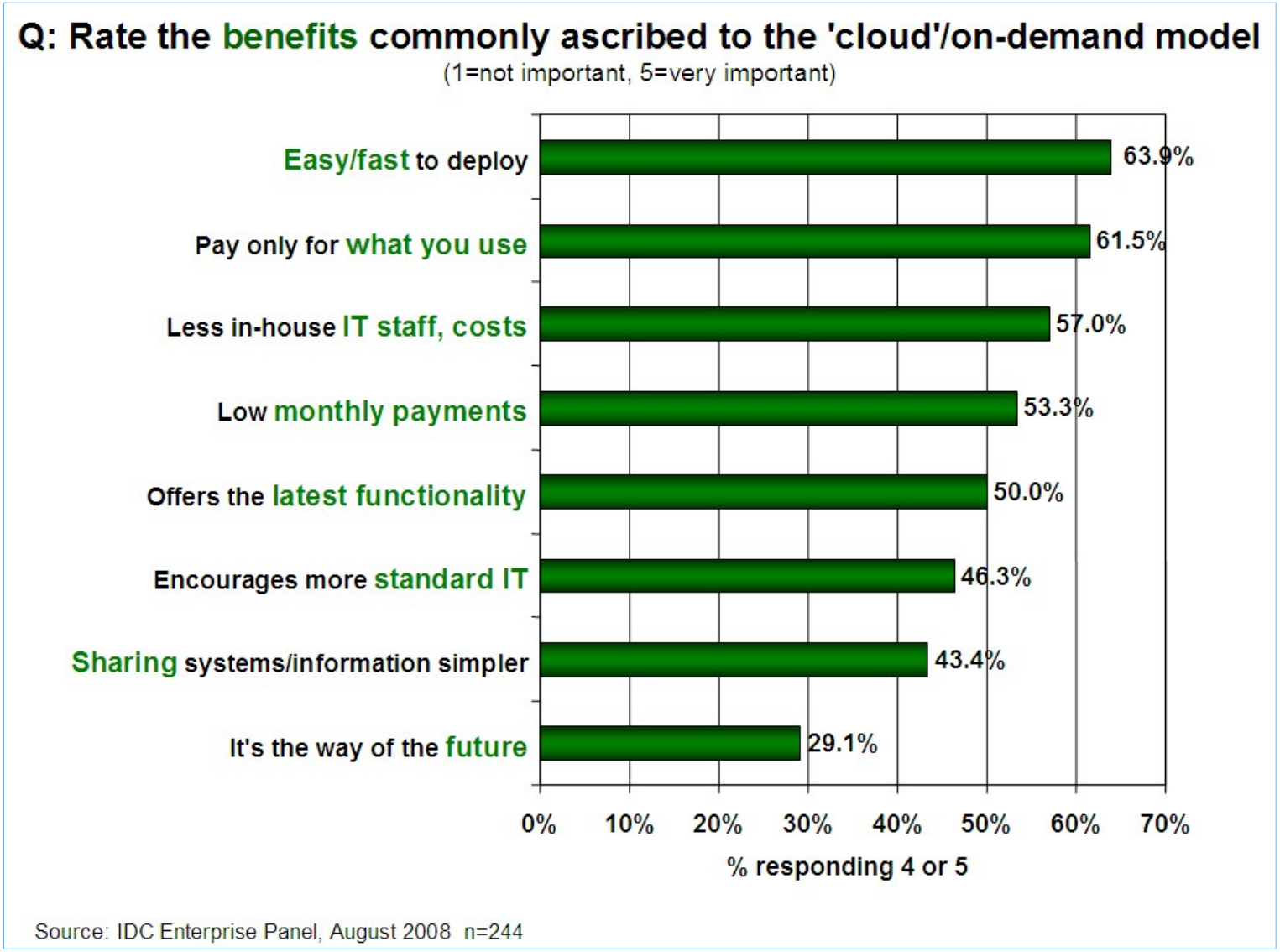
Interactive Poll – Part 1

Clearly, Cloud Computing is hot and growing at a phenomenal rate and presents organizations with some fantastic opportunities.

Question: What are the top opportunities/benefits of Cloud or on-demand computing for your agency or department?

Priority	Opportunity/Benefit
1.	
2.	
3.	
4.	
5.	

Interactive Poll – Part 1 – Survey Results



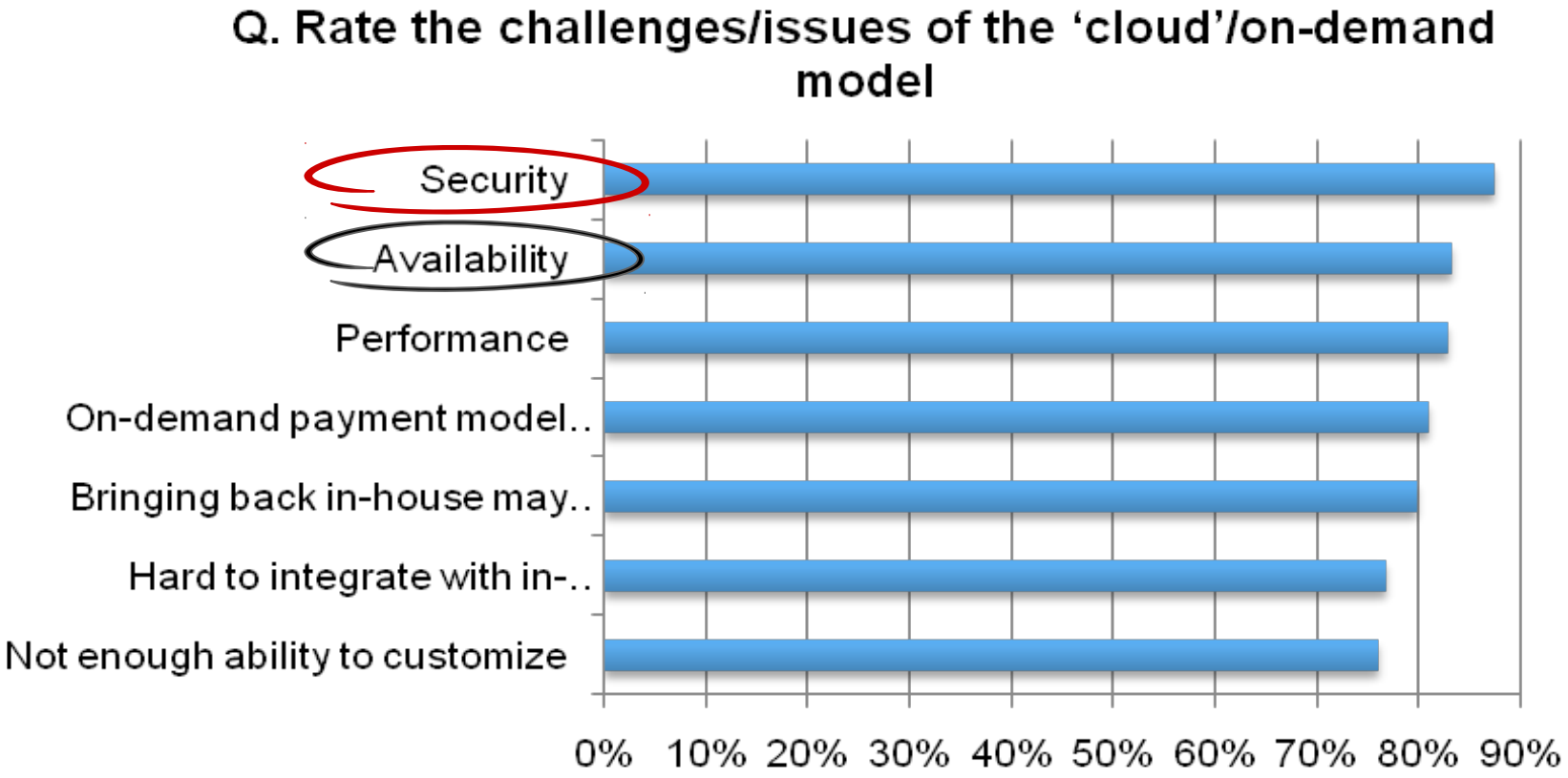
Interactive Poll – Part 2

- **However, implementing Cloud Computing also presents organizations with some significant issues and challenges.**

- **Question: What are the top issues/challenges of Cloud or on-demand computing for your agency or department?**

Priority	Issues/Challenges
1.	
2.	
3.	
4.	
5.	

Interactive Poll – Part 2 – Survey Results

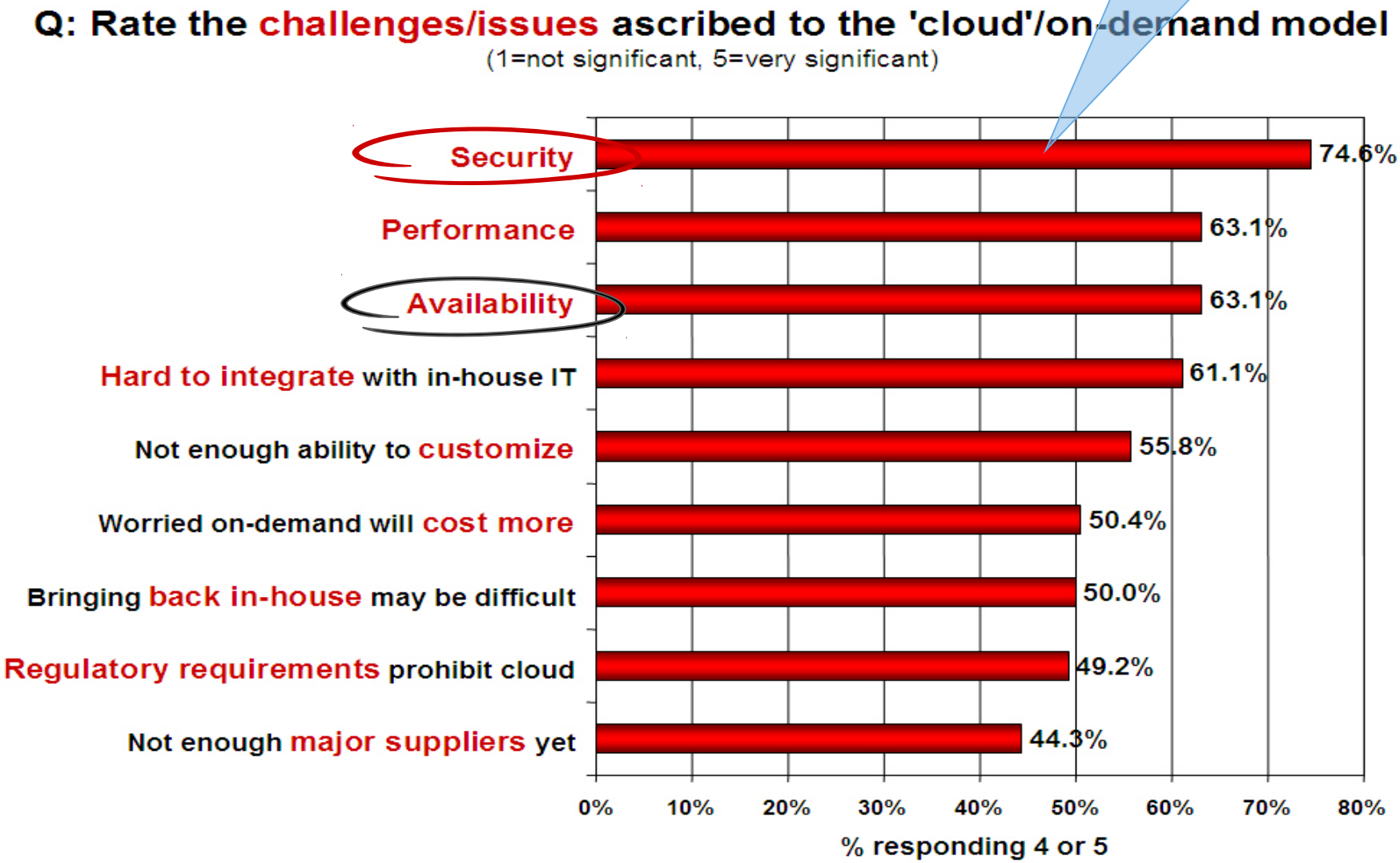


*Scale: 1= Not at all concerned 5=Very concerned

Source: IDC Enterprise Panel, 3Q 09.n=263, September 2009

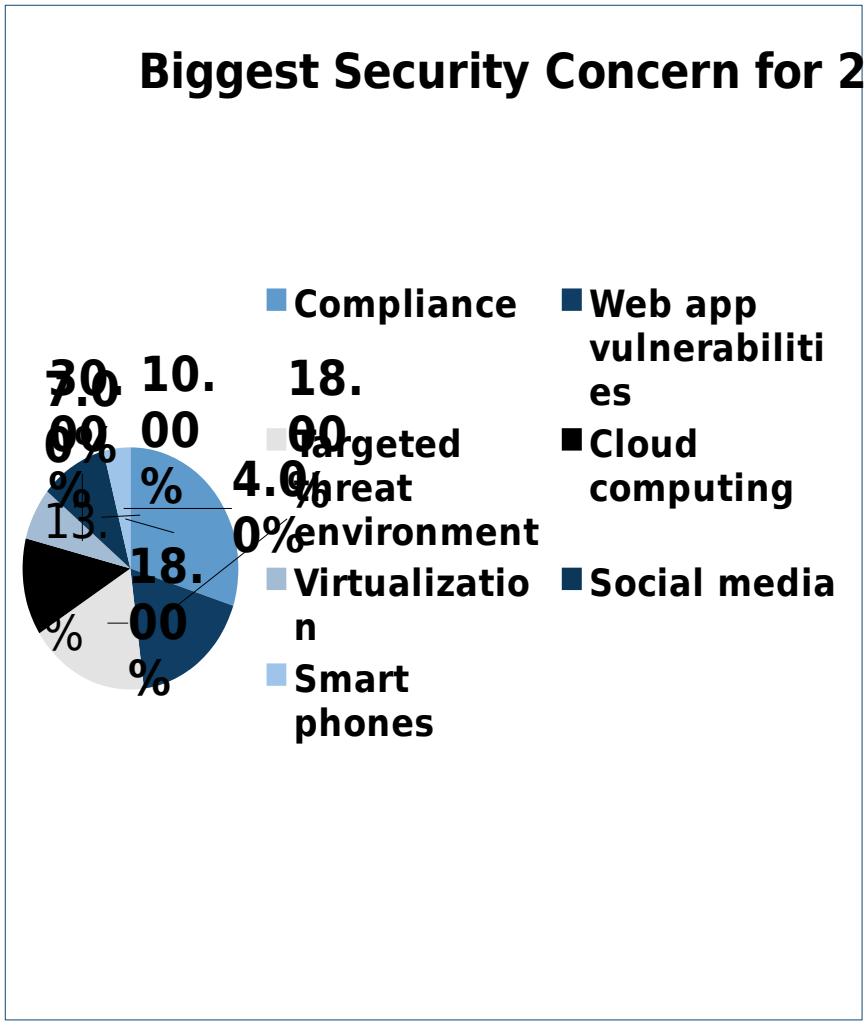
Interactive Poll – Part 2 – Survey Results

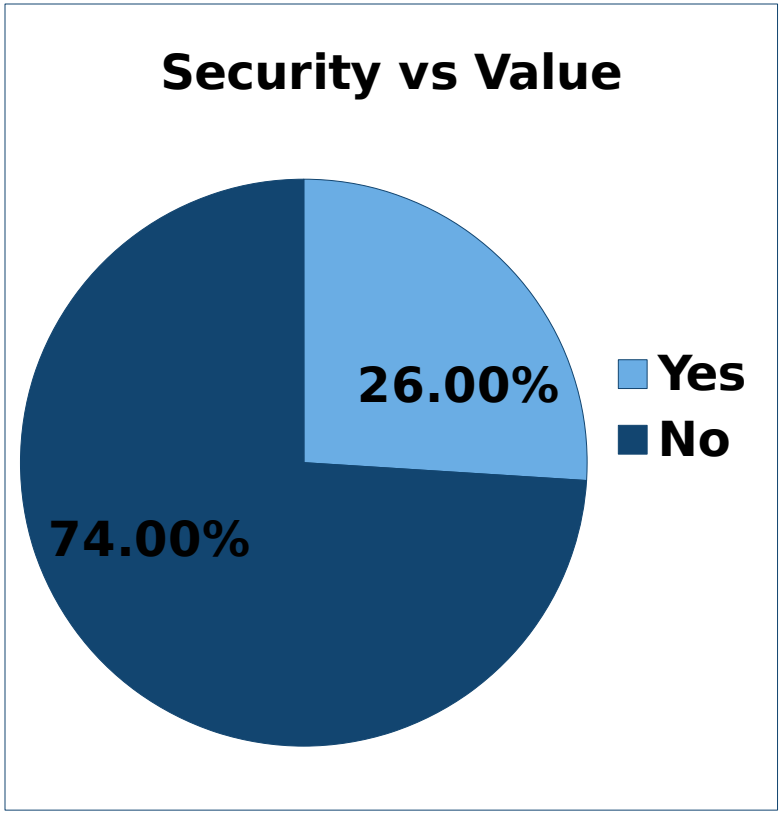
Pick your Cloud survey … any survey … they all look like this!



Source: IDC Enterprise Panel, August 2008 n=244

Some 2010 Survey Data





Does the cost savings of cloud computing outweigh security considerations for your organization?

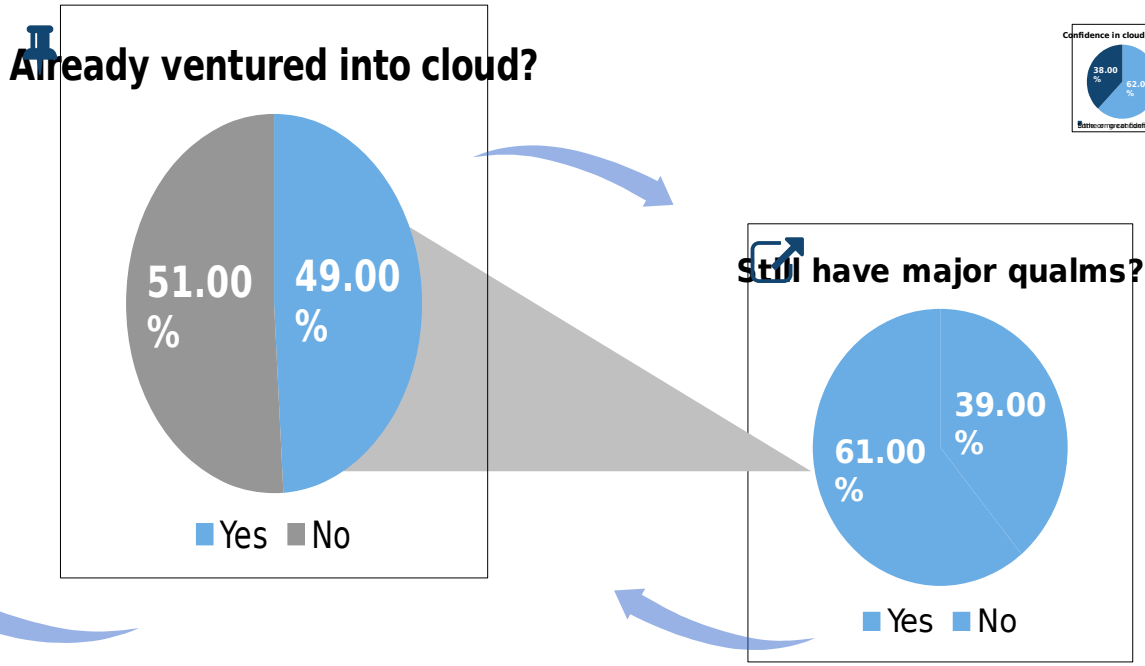
Source: nCircle **2010 Information Security & ComplianceTrend Study**

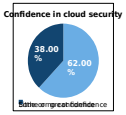
Over and over again …

Today's issues with cloud security …

- Uncertain about the ability to enforce security policies at a provider site
- Inadequate training
- Inadequate auditing

- Regulatory needs:
  - guidelines for which kinds of data it is acceptable to store in the cloud
  - Clarification on how financial reporting controls should work in the cloud





Source: Eighth Annual Global Information Security Survey
CIO, CSO, PriceWaterhouseCoopers (Sept 2010)

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

Novell Finds Widespread Concern About Cloud Security

Even so, adoption of public and private cloud computing is higher than anticipated and will continue to grow, finds survey.

By Mathew J. Schwartz
InformationWeek
October 5, 2010 12:42 PM

"Nine out of 10 cloud computing users remain concerned about **cloud security**, yet 77% of businesses already use some form of cloud computing.

Those findings come from a survey conducted by Harris Interactive for Novell, ...

But from a **security standpoint**, related concerns are a primary barrier to cloud computing adoption for 50% of respondents. Indeed, 76% think that **private data is more secure** when stored on the premises, rather than with a vendor, and 81% worry about maintaining **compliance** with regulations if they store sensitive data in the cloud.

Even with such security concerns, however, according to Novell, the survey found "**much broader adoption** of cloud computing than has been suggested by previous research, and shows **accelerating momentum** behind developing private cloud infrastructures."

Today, for example, about one-third of organizations already use a mixture of private and public clouds, and 43% intend to further increase their use of this combination. Furthermore, 87% see clouds living in harmony with corporate data

Source: http://www.informationweek.com/news/security/storage/showArticle.jhtml?articleID=227700

NASA CTO discusses Cloud Computing and Security

- “I really believe the cloud can be **more secure** than what we do today because they spend more resources, they have certainly a lot of redundancy, and redundancy comes in all shapes and sizes and it's fairly uniform so if you apply a patch, you can apply to everything at once. That is different than our internal data center. **I believe [the cloud] can be more secure at one point.”**
  - Tom Soderstrom, CTO at NASA's JPL

http://www.govinfosecurity.com/articles.php?art_id=3177&rf=2010-12-20

The Conversation

- ✓ Why are we here? Because Cloud Computing is Hot!
- ✓ A very brief overview of “Cloud Computing”
- ➢ Federal Government and Cloud Computing
- Cloud Computing Strategy
- Cloud Computing Security Considerations

Cloud Computing and the Federal Government

- Federal Data Center Consolidation Initiative (FDCCI)
- OMB 25 Point Plan
- Federal Cloud Computing Strategy
- FedRAMP
- Cloud Computing Case Studies in the Federal Government

"The cloud will do for government what the Internet did in the '90s. We're interested in consumer technology for the enterprise. It's a fundamental change to the way our government operates by moving to the cloud. Rather than owning the infrastructure, we can save millions."

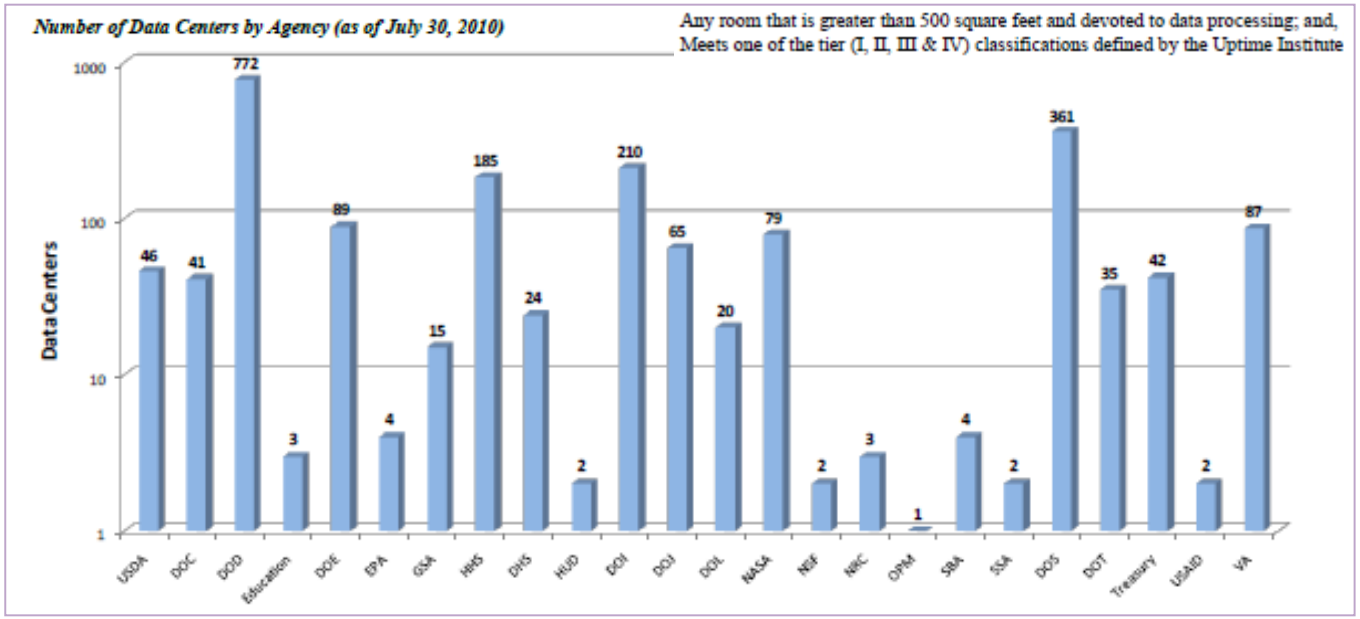
Vivek Kundra (Federal CIO)
http://www.nextgov.com/nextgov/ng_20081126_1117.php

FDCCI Background

- OMB launched the FDCCI in Feb 2010 to address four goals:
  - Promote the use of Green IT by reducing the overall energy and real estate footprint of government data centers
  - Reduce the cost of data center hardware, software and operations
  - Increase the overall IT security posture of the government
  - Shift IT investments to more efficient computing platforms and technologies
- Agency actions required by the FDCCI:
  - Inventory current data center assets
  - Develop consolidation plans throughout fiscal year 2010
  - Integrate these plans into agency fiscal year 2012 budget submissions
- Strategic Sustainability Performance Plans (SSPP) (Sep 2010)
  - Federal CIO's commitment to reduce IT energy consumption as part of FDCCI is fully aligned with agencies SSPPs.
- Federal CIO 25 Point Implementation Plan to reform Federal IT Management (Nov 2010)
  - Close a minimum of 800 data centers by 2015
  - Identify by March 2011 three "must move" services to the cloud; migrate these services and retire associated legacy systems within18 months.
  - Establish contract vehicles under GSA for commodity services (e.g., secure IaaS)

FDCCI Current Status

- OMB and agencies refine consolidation plans during 1Q FY11
- Consolidation plans finalized by end of 2Q FY11
- OMB to include agency reduction targets in FY12 budget
- Federal CIO Vivek Kundra expects agency CIOs to move to services model to renew mission focus and abstract themselves from IT
- Don’t expect additional budget to fund consolidation activities



The FDCCI Phases Which OMB Mandated In February 2010

FDCCI Phase I
Focus: Strategy & Baseline (As Is)
1Q10 - 4Q10 (Initial Submissions)
1Q11 - 4Q15 (Annual Updates)

FDCCI Phases II – IV
Focus: Analysis & Design (To Be)
1Q11 - 4Q12 (Estimated)

FDCCI Phases V – VI
Focus: Transition & Operations
1Q13 - 4Q15 (Estimated)

Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6
IT Asset Inventory Baseline	Application Mapping	Analysis & Strategic Decisions	Design & Transition Planning	Consolidation & Optimization Execution	On-going Optimization Support

ACTIVITIES

- Create an inventory of HW/SW assets by data center
- Capture Baseline Metrics for utilization & energy for each data center
- Quick Wins

- Map Applications:
  - ✓To Server/Mainframe
  - ✓To Database/Platform
  - ✓App Dependencies
  - ✓App Security
  - ✓App Usage & SLAs
  - ✓Segment Architecture

- Perform energy and cost evaluation of different approaches
- Identify the risks, alternatives, cost assumptions and business benefits
- Make strategic technology & consolidation investment decisions

- Design & test consolidation alternatives
- Develop transition plan for energy use optimization & data center consolidation
- Create project plan and WBS for the transition plan

- Execute virtualization, consolidation and migration plans
- Execute energy use optimization plans
- Measure and report on Utilization and Cost Savings Metrics

- Continue energy use optimization, virtualization and consolidation
- Continue on-going monitoring and reporting of Utilization and Cost Savings Metrics

DELIVERABLES

1	2	3	4	5	6
IT Asset Inventory Baseline & Quick Wins	*Application Mapping*	*Consolidation Analysis & Strategic Investment Decisions on Standard Platforms and Services*	*Consolidation Design & Transition Plan*	*Consolidation Execution & Progress Reports*	*Semi-annual Metrics Reports*

OMB 25 Point Implementation Plan to Reform Federal IT Mgmt
Overview

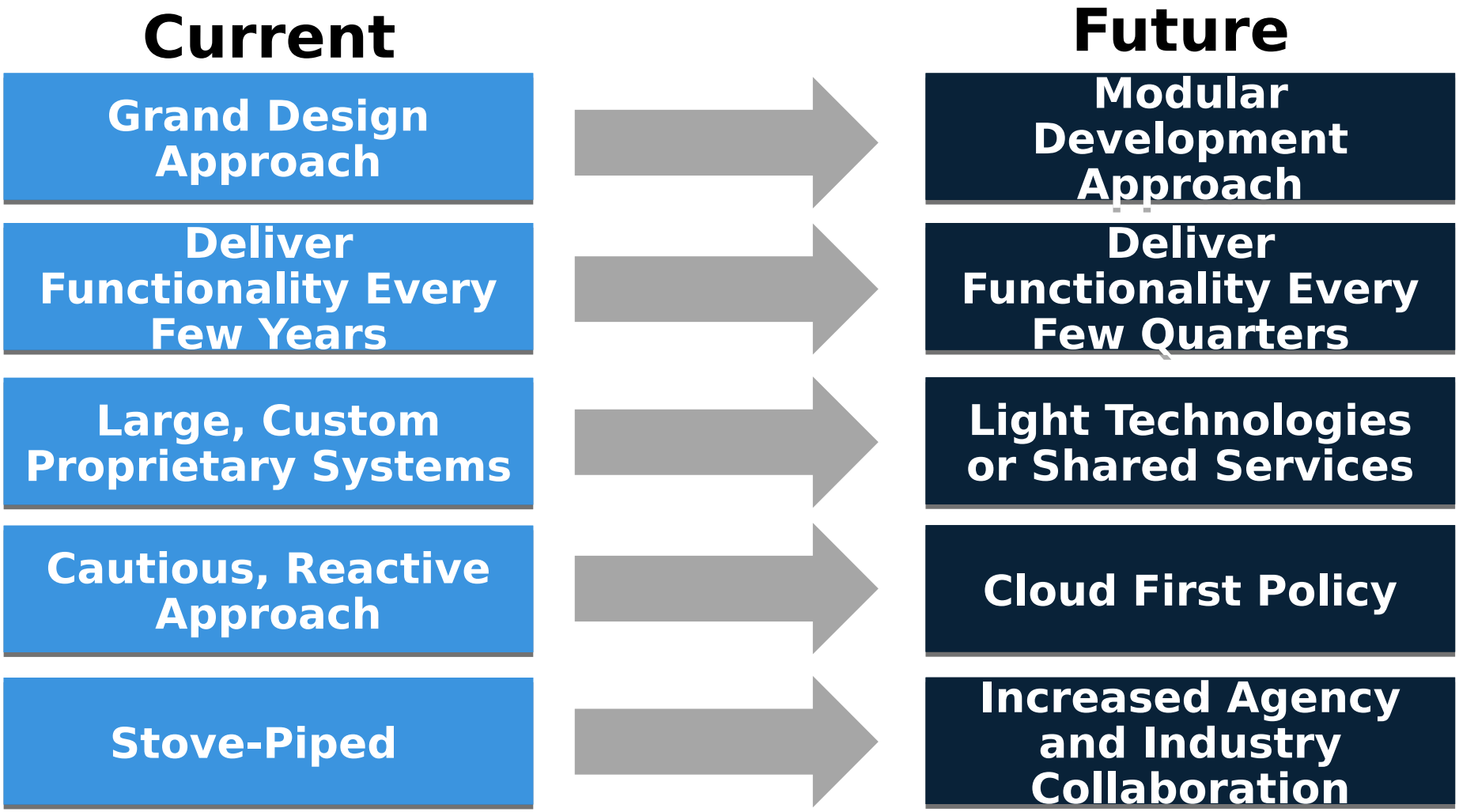
- Announced December 9, 2010, by Federal Chief Information Officer Vivek Kundra
  - Action plan to deliver results to taxpayers in the next 18 months
  - Places ownership with the OMB and agency operational centers
  - Contains 25 specific actions associated to timelines with assigned ownership; actions are divided into 2 sections and grouped into 1 of 6 categories

- Purpose: **Clear obstacles to allow Federal agencies to leverage IT to create a more efficient and effective government**
  - Enable better service delivery with enhanced collaboration with citizens
  - Incr
  - Dra cies

VISION: **More nimble, more cost effective, and more citizen-focused government**

OMB 25 Point Implementation Plan to Reform Federal IT Mgmt

The Movement to a New Federal IT Environment



xxx, 2010

OMB 25 Point Implementation Plan to Reform Federal IT Mgmt

Highlights

OMB 25 Point Implementation Plan to Reform Federal IT Mgmt
Plan Structure

- Divided into two sections
  - **Achieving Operational Efficiency** - cloud solutions and leverage shared services; 6 total actions
  - **Managing Large-Scale IT Programs Effectively** – structural areas that impact the success of large IT programs; 19 total actions

OMB 25 Point Implementation Plan to Reform Federal IT Mgmt

1 - Apply Light Technology and Shared Solutions

1. Complete detailed implementation plans to consolidate at least 800 data centers by 2015
2. Create a government-wide marketplace for data center availability
3. Shift to a “Cloud First” policy
4. Stand-up contract vehicles for secure IaaS solutions
5. Stand-up contract vehicles for commodity services
6. Develop a strategy for shared services

Federal Cloud Computing Strategy
Cloud First Policy

Problem Statement

"The Federal Government's current Information Technology (IT) environment is characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times. These inefficiencies negatively impact the Federal Government's ability to serve the American public."

Solution

"Cloud computing has the potential to play a major part in addressing these inefficiencies and improving government service delivery. The cloud computing model can significantly help agencies grappling with the need to provide *highly reliable, innovative services quickly despite resource constraints*."

IT Policy

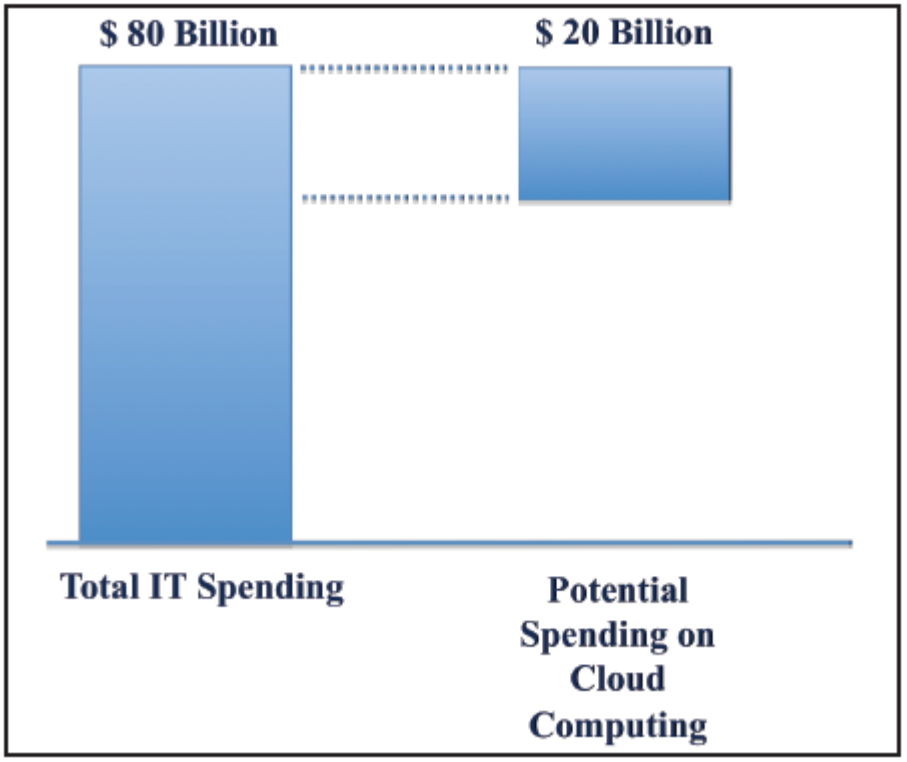
"To harness the benefits of cloud computing, we have instituted a Cloud First policy. This policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments."

Vivek Kundra, Federal CIO
February 8, 2011

www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

Federal Cloud Computing Strategy
Potential Spend on Cloud

Figure 1: Estimated portion of Federal IT spend able to move to the cloud

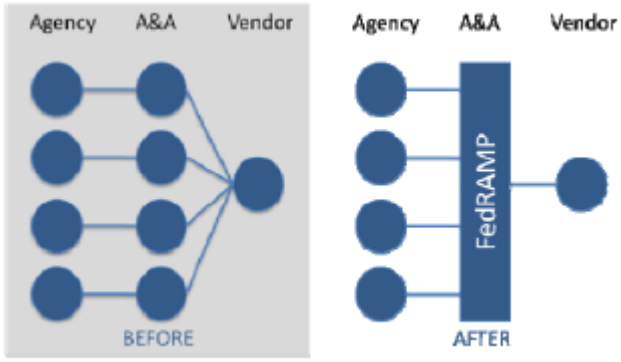


www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

FedRAMP

Federal Risk and Authorization Management Program (FedRAMP) is an interagency effort led by the General Services Administration (**GSA**), under the authority of the Federal Chief Information Officer (CIO), and with joint authorization support from the Department of Homeland Security (**DHS**), Department of Defense (**DOD**) and **GSA**.

FedRAMP provides a **standard approach** to Assessing and Authorizing (A&A) cloud computing services and products. FedRAMP allows joint authorizations and continuous security monitoring services for Government and Commercial **cloud computing systems** intended for multi-agency use. Joint authorization of cloud providers results in a **common security risk model** that can be **leveraged** across the Federal Government. The use of this common security risk model provides a **consistent baseline for Cloud based technologies** which enables the government to "approve on ensuring multiple agencies gain the benefit an FedRAMP's Authorization and access to service packages.



The first phase of FedRAMP is expected to be operational **first quarter CY2011**.

tp://www.cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedR

The Federal Government and Cloud Computing - Summary

- In consideration of these mandates and policies…
  - FDCCI
  - OMB 25 Point Implementation Plan
  - CloudFirst Policy
  - Federal Cloud Computing Strategy
  - FedRAMP
  - …

- "We've all received our cloud marching orders, but OMB mandates are not the only reason to move forward. **Cloud computing is a step forward in addressing the really big challenges we face**: budget and deficit crises, increasing greenhouse gas emissions, and a population in need of critical government services."
  - Mary Davie, Assistant Commissioner, GSA FAS Office of Integrated Technology Services

http://gsablogs.gsa.gov/technology/

SaaS in Government

- Cloud Email
  - Google Apps for Government
    - GSA, City of Los Angeles, City of Orlando, Washington DC
  - Microsoft BPOS-Federal (Office 365)
    - USDA, 120,000 users
- Email Security
  - Microsoft Forefront Security
  - Google Message Security (Postini)
- Productivity Apps
  - Google Docs
  - Microsoft Office 365 - Sharepoint, Live Meeting, OCS
- Customer Relationship Management
  - Microsoft Dynamics
  - Salesforce.com
    - Census 2010

Case Study: SaaS in Government – DISA Enterprise E-Mail

The U.S. Army hopes to **save $100 million** annually by moving from its current network of many disparate e-mail systems to one enterprise system hosted by DISA in what Army CIO and Lt. Gen Jeffrey Sorenson said … is just the first step in a much wider military email consolidation effort.

Currently, the Army spends about $400 million annually on e-mail, administering innumerable isolated e-mail instantiations all around the world running different instances and sometimes different versions of Microsoft Exchange and Active Directory.

The new effort, inked in a September deal with DISA … would result in one toll-free enterprise service desk and one shared enterprise email service for **1.4 million** common access card users in the Army. Instead of spending more than $100 per seat per year, the new deal will cost the Army **less than $39 per seat per year**.

DISA
DEFENSE INFORMATION SYSTEMS AGENCY
DEPARTMENT OF DEFENSE

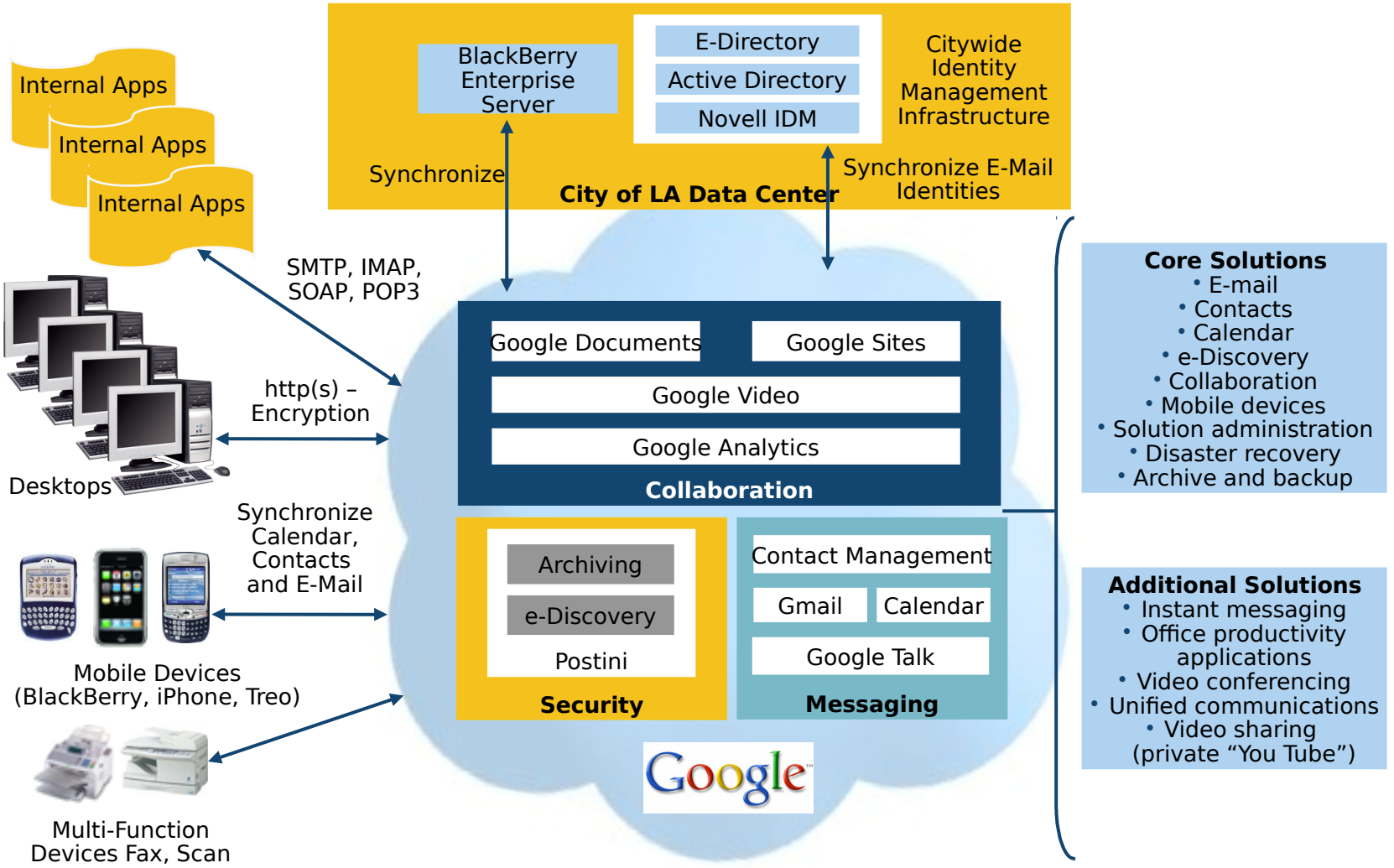
http://www.informationweek.com/news/government/enterprise-apps/showArticle.jhtml?articleID=22790

Case Study: SaaS in Government – City of Los Angeles GEECS

- City of Los Angeles
  - 2nd largest city in the US: 3.6M residents
  - Over 40 City departments and 35,000 employees
  - Annual budget of $6.7 billion
  - FY2008-09 projected $400 million shortfall
- Google Enterprise Email and Collaboration Suite (GEECS)
  - In 2009, LA spends approximately $500 million per year on technology and the Mayor charged CTO with reducing $15-20M in city-wide IT spending
  - Retiring the Novell GroupWise system and implementing the Google SaaS email and collaboration service is the key cornerstone to attaining this goal
  - Security concern: physically separated environment for government only, with a logical separation between agencies
  - Implemented Google Apps for Government (GAGE) to address LA's security and functional requirements
- ROI
  - $7.2M Program over 5 years
  - $5.5M hard-cost savings (eliminate 92 servers)
  - $20M soft-cost savings

Google™

Case Study: SaaS in Government – City of Los Angeles GEECS



Integration with existing components and an innovation platform

Case Study: SaaS in Government – NASA Shared Services Center

NASA has moved its citizen-support center to the cloud to cut costs by reducing call-center inquiries. NASA is now using the RightNow Technologies' Secure Government Cloud to run its NASA Shared Services Center, a public/private partnership with Computer Sciences Corp. that provides financial management, human resources, IT and procurement services to the space agency, according to RightNow.

The NSSC contact center last year on average received 7,000 monthly calls, and RightNow CX -- a suite of customer-experience applications -- now will be fielding those, the cloud infrastructure provider said. People can use the self-service application on the NSSC Web site to help find online answers to questions for which they would otherwise use a call-center attendant.

RightNow's cloud has achieved compliance with Federal I Security Management Act (FISMA), a National I Standards and Technology (NIST) security standard for IT products and solutions deployed in the federal

http://www.informationweek.com/news/government/cloud/saas/showArticle.jhtml?articleID=2291003

Case Study: SaaS in Government – Census 2010

The US Census Bureau was in need of Customer Relationship Management (CRM) software to coordinate and track partnership activities between the Census Bureau and outside organizations to record, track, and manage partner contacts and activities between various geographically distributed Census staff.

To meet this need, the US Census Bureau selected a solution provided by Salesforce.com. The Census Bureau appreciated that Salesforce.com required no installation or plug-ins be downloaded to these staff PCs. This meant that the Census Bureau was able to avoid coordination of a complex and costly software rollout to remote staff.

The Integrated Partner Contact Database (IPCD) project (Salesforce/Acumen/CRM) was rapidly implemented in 12 weeks for the first phase of users, in order to be functional for operation on the decennial census. The Census Bureau will deploy up to 2,200 users on the Salesforce CRM application at the projects' peak, and the[illegible]l be us[illegible]e to directly manage the partnership activ[illegible] 2010 decennial census.

http://www.siia.net/saasgov/2009/studies_detail.asp?ID=4

PaaS in Government

- Gartner Says 2011 Will Be the Year of Platform as a Service
  - All the leading enterprise software vendors, as well as large cloud specialists, will introduce new platform-as-a-service (PaaS) offerings this year, making 2011 the year of PaaS. These leading vendors are expected to deliver new or strongly expanded PaaS service offerings and cloud-enabled application infrastructure products.
- GSA conducting market research on PaaS
- PaaS Examples
  - Google App Engine platform
  - Microsoft Azure platform
  - Force.com platform
- Database as a Service (DBaaS)
  - Microsoft: SQL Azure
  - Salesforce.com: Database.com - SAS 70 Type II, SysTrust, and ISO 27001
  - Amazon.com: Amazon Relational Database Service (RDS)

http://www.gartner.com/it/page.jsp?id=1586114

Case Study: PaaS in Government – Department of State

- The State Department's Nonproliferation and Disarmament Fund (**NDF**), established in 1994, provides a means for the US government to respond rapidly to nonproliferation and disarmament opportunities, circumstances or conditions that are unanticipated or unusually difficult, but of high priority. DoS used **Salesforce.com's Force.com platform** to create a **custom application** to provide program managers around the world with ready access to up-to-date budget information. This **increased productivity** while enabling NDF to better manage contractor costs.
  - Improved technology management. Using Force.com, the NDF was able to deliver the application at **less than a quarter of the time and cost** that would have been required with traditional on-premise development environments.
  - Increased productivity. **Ready access to information** enables program managers to make decisions more quickly and plan program initiatives.
  - Better contractor management. **Better visibility** into contr[illegible]d project details on an ongoing basis enables program manag[illegible] run projects in a more hands-on fashion to **reduce the time and cost of changes and increase overall efficiency.**

https://www.salesforce.com/assets/pdf/casestudies/State_Department_Case_Study_Final_Nucleus_Research.pd

Case Study: PaaS in Government – USPTO

USPTO Needs

- Lower cost by simplifying maintenance and administration of web apps.
- Predictable budgeting and resource management.
- Solution based on technologies that the PTO is familiar with and can support.
- Updated look and feel that leverages modern client side technologies.
- Needing to upgrade Trademark Document Retrieval System application and web server infrastructure to address issues with stability and robustness

CSC Solution

- Redesigned Trademark Document Retrieval System using a Cloud PaaS, Google App Engine.
- Metered billing with cost quotas and automatic resource allocation.
- Industry standard frameworks, tools, and utilities from the J2EE programming language.
- Interactive site with wiki style editing of admin content (FAQ, Announcements, Help) and improved performance using AJAX.
- Scalability and reliability to provide interrupted service to a growing user population

"The system is a step forward and a good framework for the Next Generation Trademark system. I am impressed with CSC's suggestion to use the Cloud and the Google Application Engine to develop this solution." David Kapos, Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office, 10/27/2010

Case Study: IaaS in Government – GSA contract

- GSA IaaS contract

Apps.gov to Feature Storage, Virtualization, and Web Hosting Solutions

October 19, 2010

WASHINGTON – The U.S. General Services Administration announced today that federal, state, local, and tribal governments will soon have access to cloud-based Infrastructure as a Service (IaaS) offerings through the government's cloud-based services storefront, Apps.gov. GSA's IaaS contract award allows vendors to provide government entities with cloud storage, virtual machines, and Web hosting services to support a continued expansion of governments' IT capabilities into cloud computing environments.

Case Study: IaaS in Government – Treasury.gov

The new Treasury.gov

By: Dan Tangherlini , 12/6/2010

"I'm proud to announce the launch of the completely rebuilt and redesigned online home of the Department of the Treasury. We've worked hard to make it easier for citizens like you to find the information you need while upgrading the technology that powers the site so that we can offer more while saving taxpayers money.

"And for those of you interested in some of the improvements we made under the hood, here are some additional facts about the new site.

- *Cloud Infrastructure* – Treasury is now the first cabinet-lev have its website fully hosted in a public "cloud," a substa cost-efficient hosting solution.
- Microsoft SharePoint 2010 platform
- A Compute Cloud (EC2)
- Akamai Content Delivery Network

http://www.treasury.gov/connect/blog/Pages/The-new-Treasurygov.aspx

Case Study: IaaS in Government – DISA RACE

The Rapid Access Computing Environment (RACE) service provides a streamlined process for the provisioning and subsequent development, testing, certification and accreditation and deployment of applications to a DISA Defense Enterprise Computing Center (DECC). DISA CSD provides hosting, networking, security and connectivity, and offers the package to DoD Customers as a service. RACE is available to all DISA CSD Customers, including all Services and Agencies, as well as their corporate design partners. Users can acquire server capacity rapidly, for short or long-term use, using Operations and Maintenance (O&M) or Research, Development, Test & Evaluation (RDT&E) funding, without the need for capital acquisitions.

Case Study: IaaS in Government - Virtualization

- Lower cost of ownership through high asset utilization and reduced capital expenditures.
  - *The US Food & Drug Administration has more than 190 virtualized machines running on 3 VMware clusters, reducing server-related help-desk tickets by ~90% and increasing server utilization from 5-10% to 55-60%.*
- Simplified provisioning and deployment, cutting time to release new services from perhaps six or more months to hours or even days.
  - *Through virtualization, the Defense Contract Management Agency (DCMA) eliminated 400+ physical servers, achieved a $1.5M annual cost avoidance, and reduced server deployment time from 4 weeks to 15 minutes.*
- Reduced systems and infrastructure management through ubiquitous automation.
  - *The Navy-Marine Corps Intranet (NMCI) consolidated 2,000 [illegible]cal [illegible]nto 3[illegible]ervers while m[illegible]ning consistent computing capabilities and service levels. Power and cooling costs were reduced by 65%, saving NMCI $1.6M annually.*

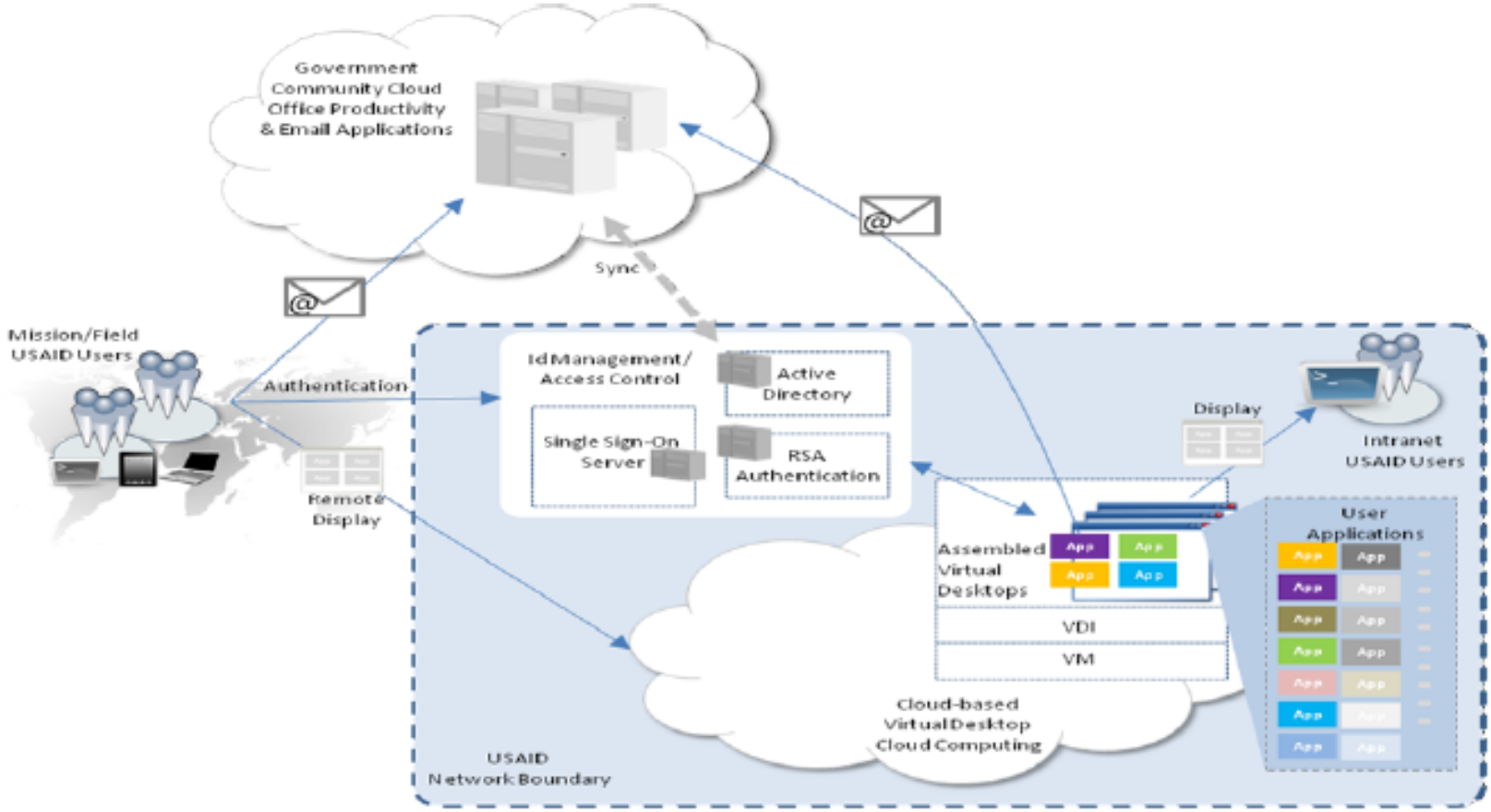
vmware

U.S. Food and Drug Administration
Protecting and Promoting *Your* Health

Federal Roadmap to the Cloud, A VMware Federal White Pape

Case Study: IaaS in Government – USAID Desktop Virtualization

- USAID Virtual Desktop – NIST has a White Paper describing the progress at USAID in moving to the cloud



http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/USAIDVDIBUC/USAID_VDI_in_the_Cloud

Case Study: IaaS in Government – NASA Nebula

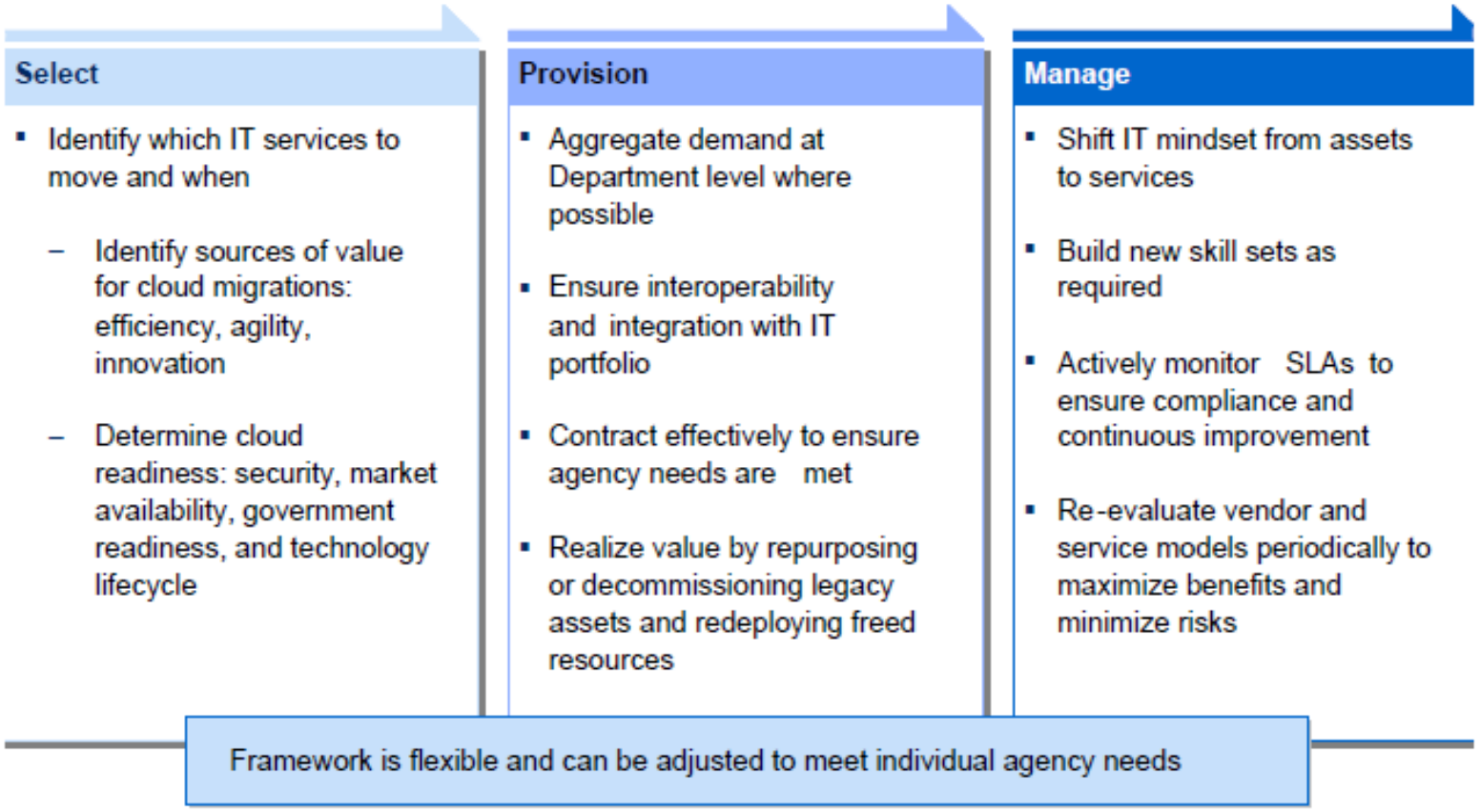
- Nebula is an open-source cloud computing project and service developed to provide an alternative to the costly construction of additional data centers whenever NASA scientist or engineers require additional data processing. Nebula also provides a simplified avenue for NASA scientists and researchers to share large, complex data sets with external partners and the public.
  - **Compute**
    - Nebula allows scientists to launch compute resources in the form of fully functional, network-connected virtual machine instances on demand so that they can complete their research instead of developing IT solutions. Nebula's compute offering has been developed for scientific applications.
  - **Storage**
    - Nebula provides three classes of storage.
  - **Networking**
    - Nebula is currently hosted at the Ames Internet Exchange (AIX)
  - **Security**
    - Nebula developed a shared security control responsibility NIST SP 80
    and has an ATO suitable for FIPS-199 Low information

http://nebula.nasa.gov/about/

The Conversation

- ✓ Why are we here? Because Cloud Computing is Hot!
- ✓ A very brief overview of “Cloud Computing”
- ✓ Federal Government and Cloud Computing
- ➢ Cloud Computing Strategy
- • Cloud Computing Security Considerations

Federal Cloud Computing Strategy - Defining a Path Forward


Select
Identify which IT services to move and when
Identify sources of value for cloud migrations: efficiency, agility, innovation
Determine cloud readiness: security, market availability, government readiness, and technology lifecycle
Provision
Aggregate demand at Department level where possible
Ensure interoperability and integration with IT portfolio
Contract effectively to ensure agency needs are met
Realize value by repurposing or decommissioning legacy assets and redeploying freed resources
Manage
Shift IT mindset from assets to services
Build new skill sets as required
Actively monitor SLAs to ensure compliance and continuous improvement
Re-evaluate vendor and service models periodically to maximize benefits and minimize risks
Framework is flexible and can be adjusted to meet individual agency needs

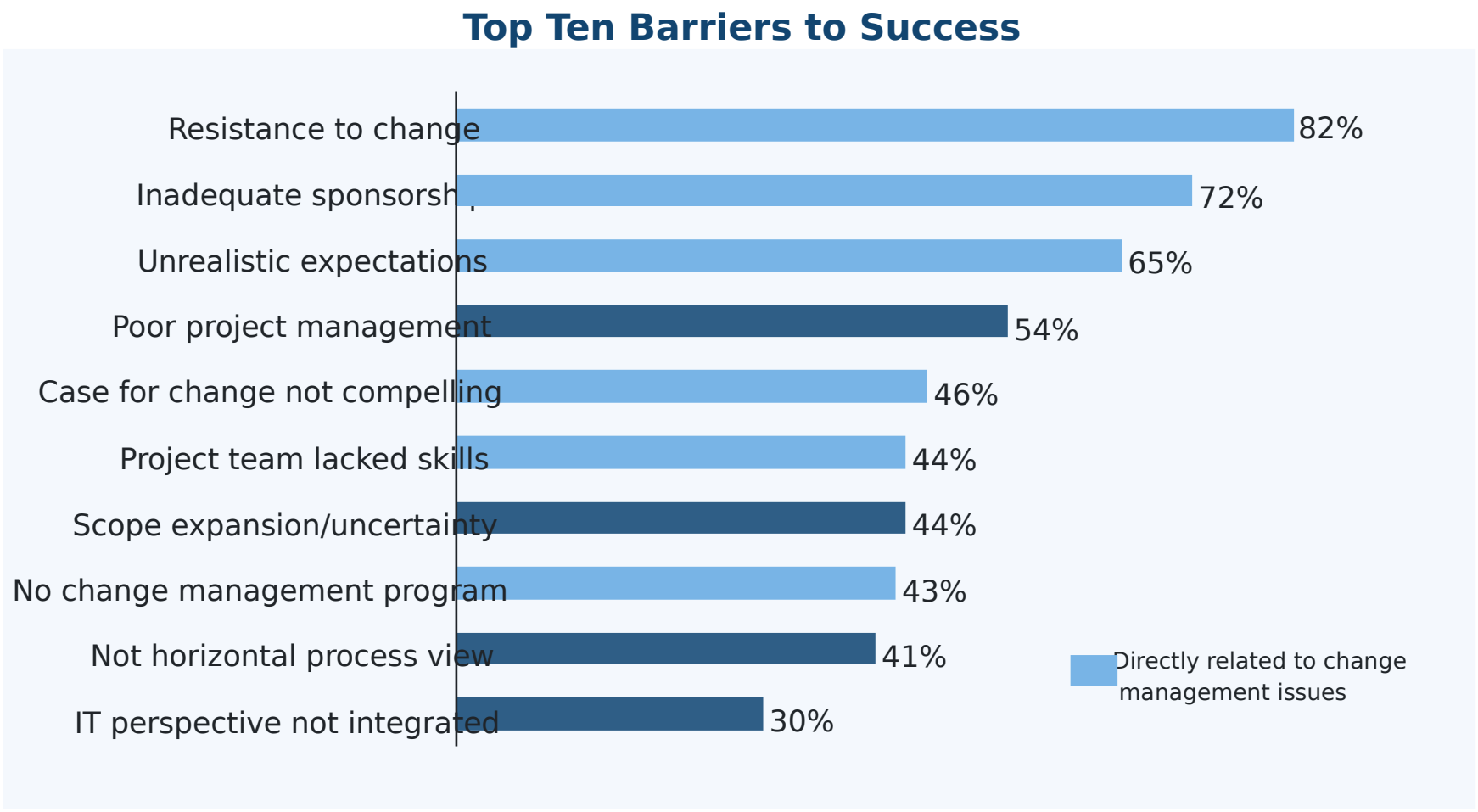
www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

NASA CTO discusses Strategy for Cloud Computing Adoption

- "Yes, so there are **three phases**."
- "There is **prototyping**, where you are really testing the waters. You haven't decided you are going to take this into operations yet. Think of it as a large funnel, lots of ideas, some of those ideas are worded to be prototype, quick results, quick measurements, but you need hands on experience."
- **"The second phase is piloting**. When we pilot something we decide, we think this is worthy of going into operations. We're going to take it through its paces, but we expect it to be into operations one day."
- "And then the **third one is into operation**. Each of those three stages cost successively more time and money."
- "But that has been a **really good approach** for us and that is one reason we have been able to **do so many things**."
  - Tom Soderstrom, CTO at NASA's JPL

http://www.govinfosecurity.com/articles.php?art_id=3177&rf=2010-12-20

MANY OF THE BARRIERS TO SUCCESSFUL CLOUD COMPUTING AND FEDERAL DATA CENTER CONSOLIDATION WILL BE CHANGE-RELATED



Source: D&T CIO Survey

WHY IT MATTERS – THE RISKS OF NOT MANAGING CHANGE

- **Integration risk** – failure to identify and factor in the interdependencies among people, process and technology
- **Sponsorship risk** – a slackening of executive commitment, focus and resource allocation
- **Buy-in risk** – failure to educate, involve and persuade key stakeholders
- **Execution Risk** – failure to deploy proper resources and hit deadlines, and translate high-level strategy into ground-level tactics
- **Retention Risk** – failure to identify and engage key talent
- **Sustainability Risk** – failure to design the systems needed to sustain change over the long haul

A CHANGE ROADMAP

Every change effort must address what people must **do**, what they **think**, and how they **feel** about what they must do

Critical Success Factors

- **Clear definition** of end game, scope, and what defines success
- Clear **ownership and visible leadership** for the execution and business outcomes of the program
- **Very close integration and coordination** of all "transformational" activities (e.g., ability to pace change across work streams)
- **Constant cross-team integration** to ensure consistent understanding and alignment
- **Strong execution and leverage of assets** in change management, governance, and solution design to enable integration and acceptance

Approach

ACTION
COMMITMENT
Visible support of all stakeholders for the change
COMMUNICATION
Key messages that define and reinforce new behaviors
CAPABILITY
Competencies and tools for success in the new environment
CONSEQUENCE
Benefits, risks and impact of doing things differently (or not).
CULTURE
Change supported through organization and business alignment
RESULTS

Harvard Study. 87% of companies who spend less than one to two million dollars on investment in a comprehensive change effort were not able to implement a successful software change even though they had spent millions on new systems and made significant investments in training

Stakeholder Enrollment Strategy

Key Stakeholders/ Position	Level of Commitment [R/Y/G]	Areas of Resistance	How to Increase Commitment?	Target Change Champion? [Yes/No] Why?

- **Stakeholder and Risk Assessment**
- **"Convert" sponsors, managers, and employees** from accepting change to leading and driving required change
- **Skills to lead change** and work in a changing environment
- **Measurement Approach**
- **Organizations reap rewards** only when change occurs at level of individual employee

Defining a Path Forward – Strategy for Adopting Cloud

Cloud adoption assessments help government define a path forward. The overall methodology is the same for all assessments, the scope, focus and key stakeholders vary, with a key goal of helping our clients manage change and achieve success in their move to the cloud.

Focused Cloud Assessment: Feasibility, process and high level financial impact of moving infrastructure and/or one or more applications or functions to the cloud.

Cloud Strategic Assessment: Organizational view as a Federal Agency, State or other large organization. This assessment focuses on creating a structure for subordinate divisions to migrate to the cloud. The focus is on policy and process to guide and standardize the migrations.

Cloud Rapid Organizational Assessment: Provides recommendations for successful business transformation, and both can be customized and scaled dependent upon the needs of the organization. It focuses on alignment of the organization and providing the technology to achieve the mission, and may include human capital management as well.

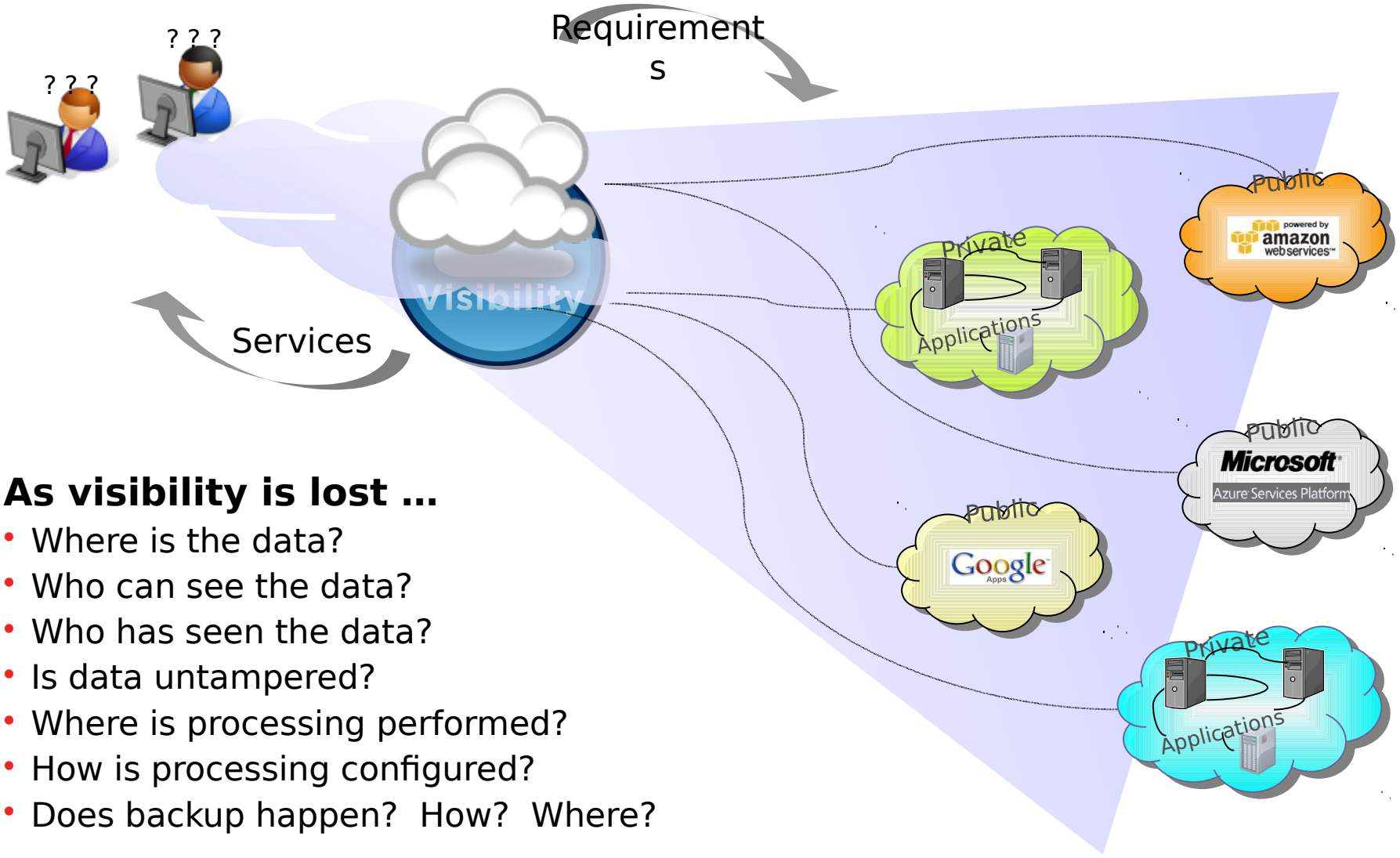
Streamlined Cloud – Process Change: Lean, business process management, and/or business process reengineering techniques may be applied to evolve the business processes to take full advantage of

The Conversation

- ✓ Why are we here? Because Cloud Computing is Hot!
- ✓ A very brief overview of “Cloud Computing”
- ✓ Federal Government and Cloud Computing
- ✓ Cloud Computing Strategy
- ➢ Cloud Computing Security Considerations

Information Assurance is Complicated

"Clouds are cloudy"



As visibility is lost …

- Where is the data?
- Who can see the data?
- Who has seen the data?
- Is data untampered?
- Where is processing performed?
- How is processing configured?
- Does backup happen? How? Where?

… Security, compliance, and value are lost as well

The Key to Effective Cloud Security – Transparency
Three Big Obstacles to Value Capture

- Lack of standards
- Lack of portability
- Lack of transparency

Leading to problems with ...

controls ..., **compliance** ..., sustained payoff ..., reliability ..., liability ..., confidentiality ..., privacy ...,

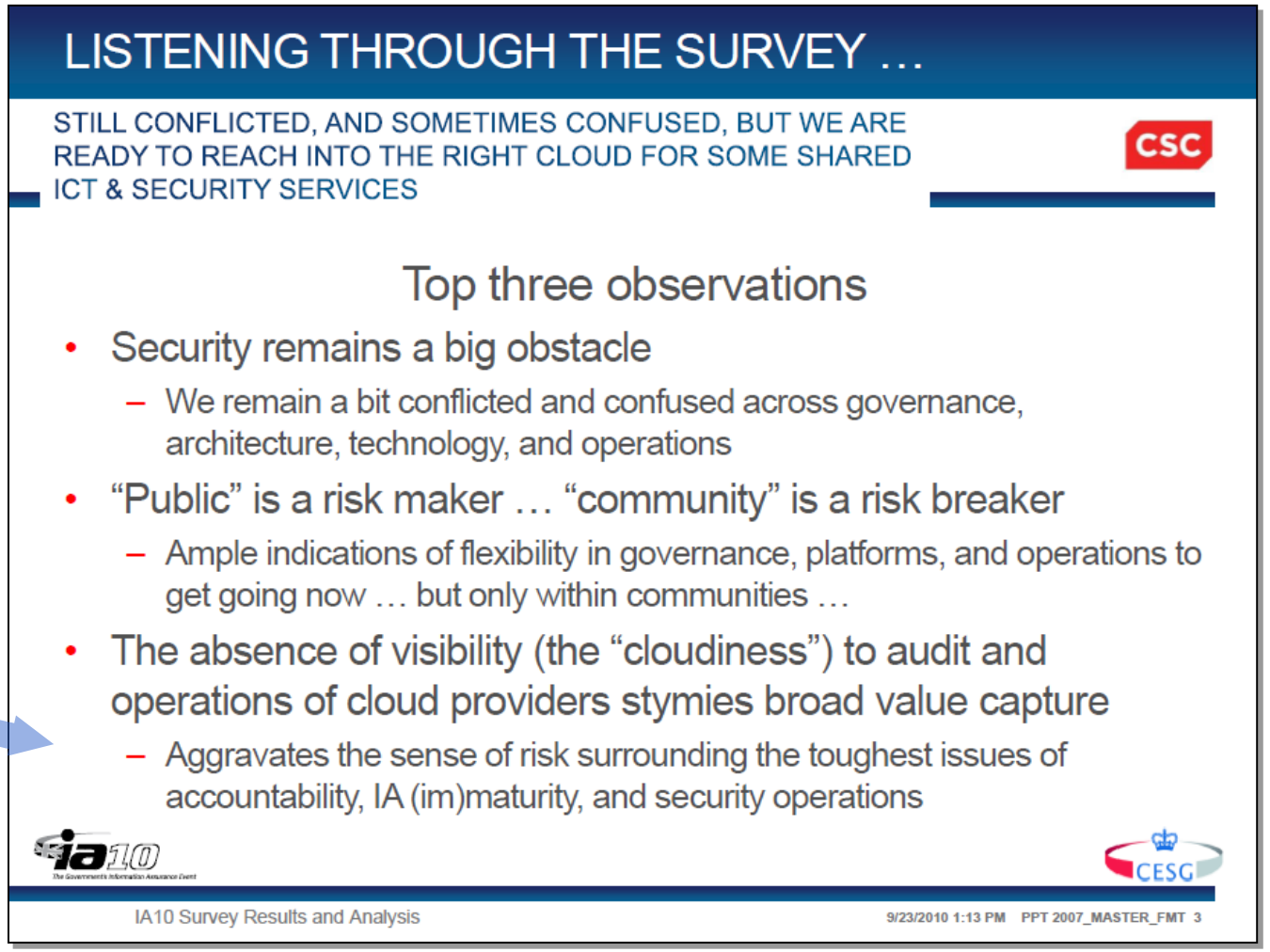
Compliance issues

• PCI DSS	• HIPAA	• **ITAR**
• ISO27001	• HITECH in ARRA 2009	• **DIACAP**
• HMG Infosec Standard 2	• GLBA	• **NIST 800-53 and FISMA**
• U.K. Manual of Protective	• FRCP	• **SAS70**

... and on and on and on ...

Transparency in the Cloud is the Key to Value Capture

- United Kingdom IA10 Conference (13-15 Sept 2010)
- Top security policy makers and providers in the UK (gov't and industry)
- Transparency is acknowledged (again) as the key to value capture


LISTENING THROUGH THE SURVEY …
STILL CONFLICTED, AND SOMETIMES CONFUSED, BUT WE ARE READY TO REACH INTO THE RIGHT CLOUD FOR SOME SHARED ICT & SECURITY SERVICES
CSC
Top three observations
Security remains a big obstacle
We remain a bit conflicted and confused across governance, architecture, technology, and operations
"Public" is a risk maker … "community" is a risk breaker
Ample indications of flexibility in governance, platforms, and operations to get going now … but only within communities …
The absence of visibility (the "cloudiness") to audit and operations of cloud providers stymies broad value capture
Aggravates the sense of risk surrounding the toughest issues of accountability, IA (im)maturity, and security operations
ia10
CESG
IA10 Survey Results and Analysis
9/23/2010 1:13 PM PPT 2007_MASTER_FMT 3

Absent Transparency … Some Big Problems

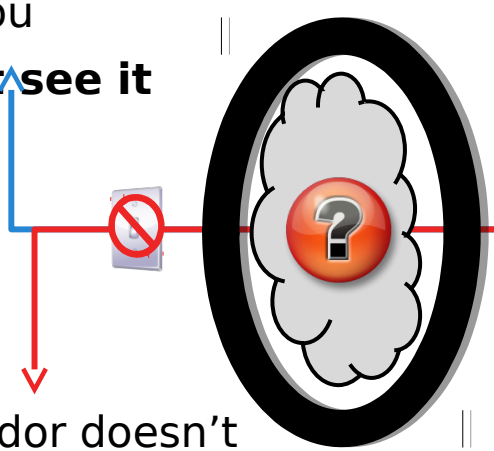
For example, … without transparency …

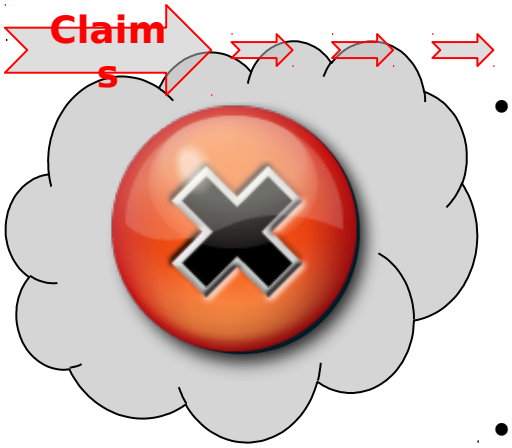
- No confirmed chain of custody for information
- No way to conduct investigative forensics
- Little confidence in the ability to detect attempts or occurrences of illegal disclosure
- Little capability to discover or enforce configurations
- No ability to monitor operational access or service management actions (e.g., change management, patch management, vulnerability management, …)

The Cloud Security Paradox
Without transparency value is lost either way!

- Cloud vendor does have all the security & privacy technologies and services claimed, and they are working now for you
- **You can't see it**

- **No Transparency?!**
- **No evidence-based confidence …!!**





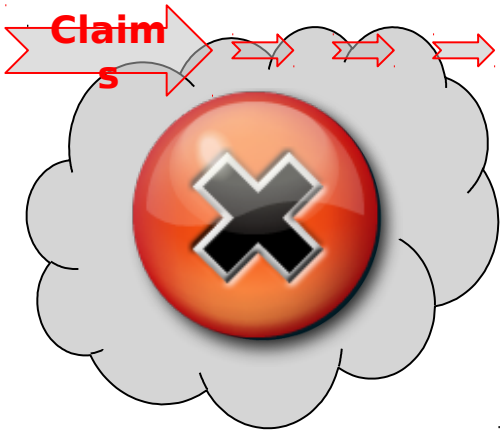
- Cloud vendor doesn't have all the security & privacy technologies and services claimed, or they are not working now for you
- **You can't see it**

Payoffs Denied

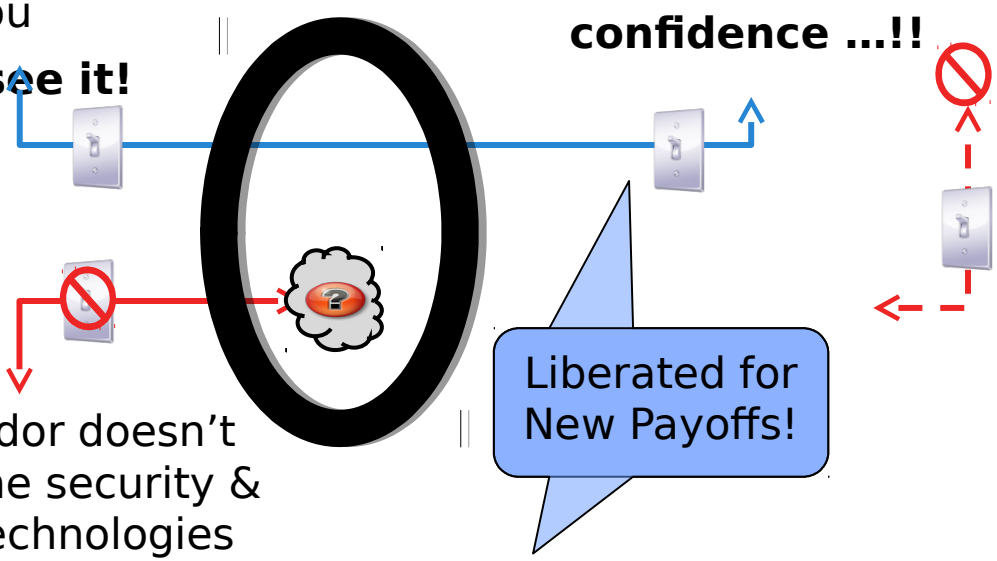
Cloud Security Starts with a ‘T’
Transparency liberates value opportunities

- Cloud vendor does have all the security & privacy technologies and services claimed, and they are working now for you
- **You can see it!**

- **Transparency!!**
- **Evidence-based confidence …!!**



- Cloud vendor doesn’t have all the security & privacy technologies and services claimed, or they are not working now for you
- **You can see it or visibility is denied**



Weatherproofing the Enterprise for Cloud Services
Transparency (monitoring) to create digital trust

Today – Compensating Approaches

Private Clouds

"Safe Computing" for Cloud Processing

Presumptive Security

Coming – Reclaiming

Transparency Services

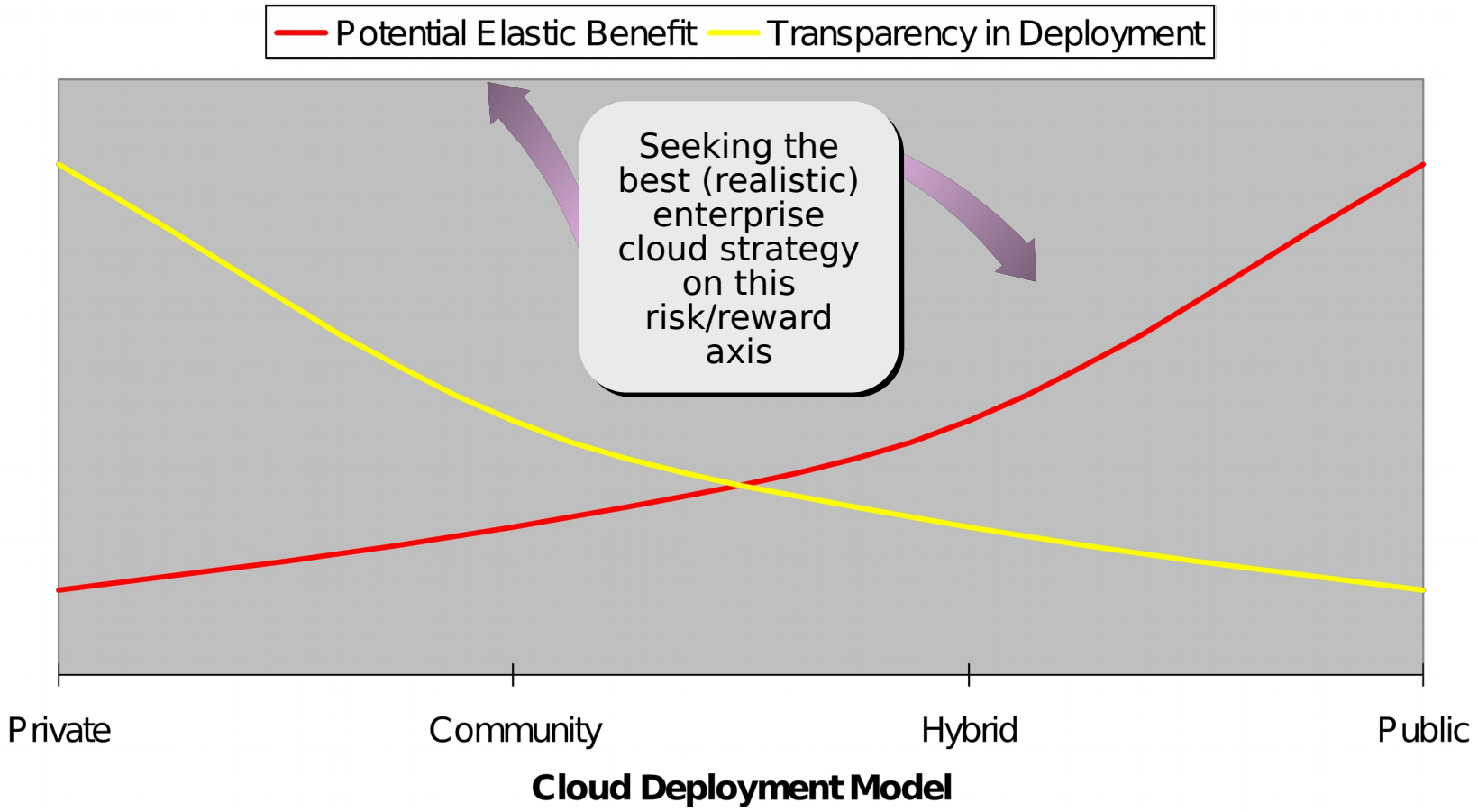
Protocols

Standards

Audits

Objective: Standards-based continuous monitoring with a purpose

Using Transparency to Ride the Payoff Curve
More applications and services become eligible for the cloud



Cloud Security in Summary…

- In summary, we want to
  - Maximize the Benefit of Cloud Computing for our organization while…
  - Ensuring Security (and CyberSecurity) of Cloud Computing by…
  - Achieving Transparency of Cloud Security.

- Cloud Security Basic Principles
  - The CIA triad
    - Confidentiality – prevent the disclosure of information to unauthorized individuals or systems
    - Integrity – ensures that data cannot be modified without authorization
    - Availability – ensures that computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly

Relevant Standards and Certifications

- Statement on Auditing Standards (SAS) 70 Type II
  - What is it? SAS 70 provides guidance to service auditors when assessing the internal controls of a service organization and issuing a service auditor’s report … A Type II service auditor’s report includes the service auditor's opinion on whether the specific controls were operating effectively during the period under review.
  - What to look for? Regularly performed audits

Relevant Standards and Certifications

- Security Plan/Policy standards
  - Implement a set of controls that cover how to run an organization (change management, oversight, hiring/firing practices, etc…) as well as how to protect technology within the organization (use of encryption, physical security, access control, etc…)
  - Federal Information Security Management Act (FISMA)
    - NIST implementing/defining via the 800 series publications
    - Various approaches: GSA accredit the solution and then make that C&A available to any agency that wants to use it (e.g. Google Apps), or an agency can accredit the solution and share that C&A with other agencies.
  - ISO/IEC 27001 explicit security certification (27k1)
    - Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
    - Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
    - Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Relevant Standards and Certifications

- Privacy/Identity
  - Access controls, who has accessed the data and why?
  - Criminal Justice Information Security (CJIS) Security Policy
    - Compliance with the CJIS Security Policy and Security Addendum will be required if any criminal justice information is sent, received, or stored …
    - Separation from non-government agencies
  - HIPAA
    - “HIPAA compliance will be required if any HIPAA related data is sent, received, or stored…”
    - Data at rest encryption

Relevant Standards and Certifications

- Security Plan/Policy standards
  - Cloud Security Alliance (CSA)
    - A non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing
      - Promote a common level of understanding between the consumers and providers of cloud computing regarding the necessary security requirements and attestation of assurance.
      - Promote independent research into best practices for cloud computing security.
      - Launch awareness campaigns and educational programs on the appropriate uses of cloud computing and cloud security solutions.
      - Create consensus lists of issues and guidance for cloud security assurance.

Relevant Standards and Certifications

- CloudTrust Protocol (CTP)
  - Mechanism to ask for and receive information about the elements of transparency that can be used to generate evidence and digital trust in the Cloud
  - Asynchronous “question and response” protocol
  - Solves two client needs for security and trust in the Cloud
    - Provides a way for clients to specify and ask about the configuration, vulnerability, access, authorization, policy, accountability, anchoring, and operating status conditions
    - Provides a way for cloud service providers to prepare and deliver information in response to requests about elements of transparency
  - The ability to respond to different CTP requests is itself a measure of the capacity to produce evidence, to create digital trust
- Security Content Automation Protocol (SCAP)
  - Method for the enumeration of configurations and vulnerabilities and for measuring differences between requested configurations

Other Cloud Data Security Considerations

- Encryption
  - Encryption of data in Transit (Network encryption) - encryption of data as it moves between the source server and destination servers(s) using SSL encryption for security. Support a minimum of 128-bit encryption which has been certified by the NIST or Canada's Communications Establishment (CSE) to ensure that cryptographic modules meet FIPS Publication140-2 for "Security Requirements for Cryptographic Modules."
  - Encryption of data at Rest - encryption of stored data.
- CONUS
  - All data generated, used or stored will reside and remain in the continental U.S. and will not be transferred outside of the continental U.S.
  - Allows litigation of security violations within US jurisdiction.
- Personnel Security Measures
  - Dependent on security policy of the organization, can include fingerprinting, criminal and financial background checks with periodic reviews for existing employees and contractors that

Other Cloud Data Security Considerations

- Authentication
  - An organization that is using a cloud service should keep in mind they are moving the authentication possibilities from being anyone on-premise to anyone on the internet, a significantly larger exposure, unless controls are put in place.
  - Depending on the data being stored there needs to be some level of control over who is able to connect/authenticate.
  - Approaches include a Single Sign-on solution, and user or IP based ACLs if the cloud provider supports them.

Other Cloud Data Security Considerations

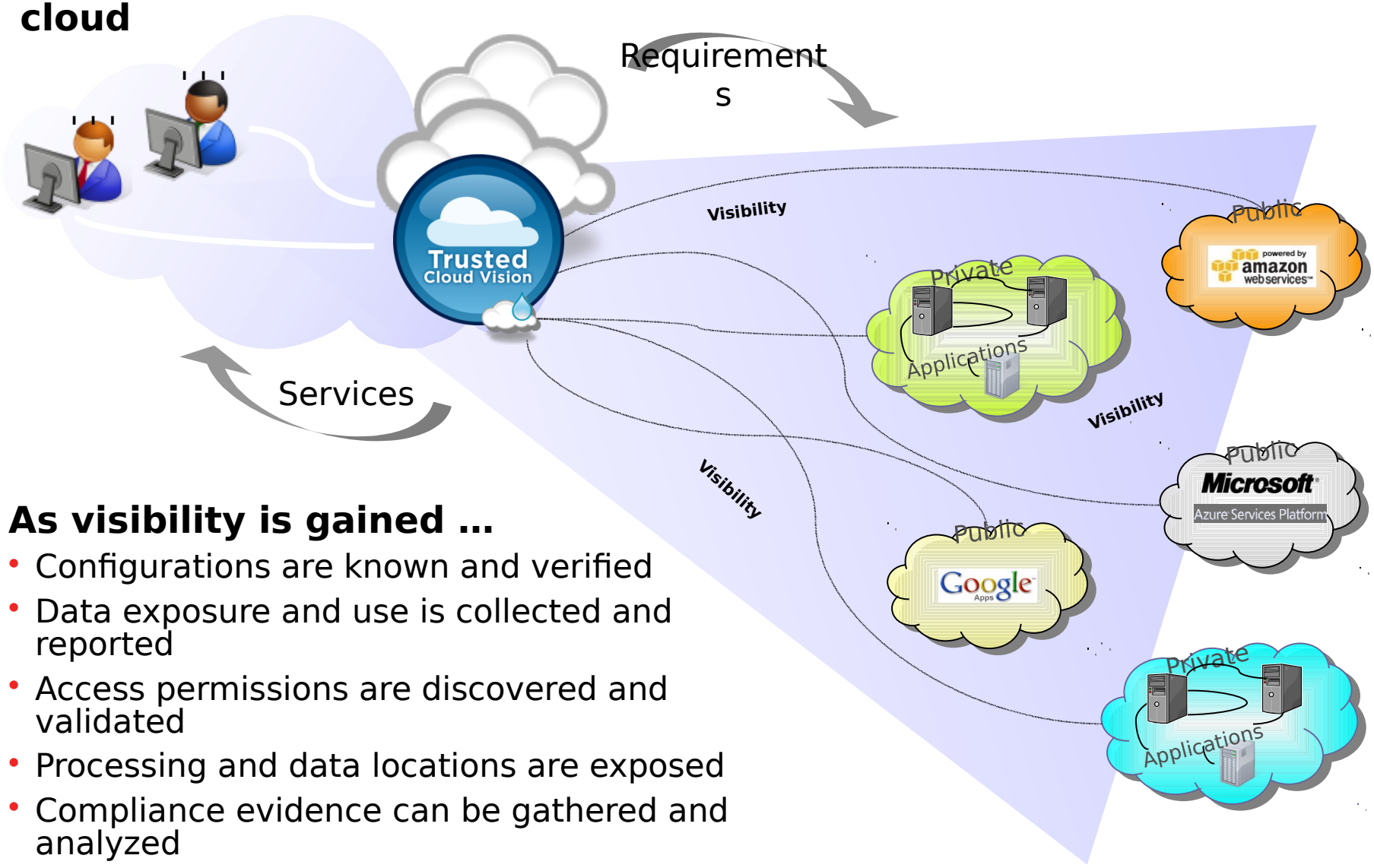
- Separation of Data
  - Ensure government data is protected and/or separated from other customer data to maintain the confidentiality and integrity of government data – compartmentalization.
    - Physical separation - Network segments may be physically separated by routers configured to prevent communications between customer managed networks and the vendor's network.
    - Logical separation - VLAN technology may be used to separate communications between customer and managed segments.
    - Firewalls – Firewalls and other network security enforcement points are used to limit data exchanges with systems exposed to the Internet and to isolate DMZ systems from backend managed systems.
    - One-way trusts - used to prevent systems or users in the Managed environment from authenticating to resources on the Management Network. A similar trust prevents these entities from authenticating to the Customer Network.
    - Protocol restrictions

Contemporary Issues and Efforts

- Standards
  - Too many to count
    - More than a dozen recognized efforts
    - Some in SDO's … some in governments … some erupting in consortia and associations or all kinds all around the world
    - Traditional SDO efforts are ponderous … so many are bypassed for now
    - Results today from cloudaudit.org (IETF experimental "protocol" recommendation)
    - CloudTrust Protocol presented as transparency protocol using (some) existing lower level protocols and standards
    - Standards efforts that do not include transparency characteristics are incomplete
  - "Best practices" (not a standard) to emerge from Cloud Security Alliance Congress in Orlando in mid-October.
  - Most public cloud providers already claim "good security"
- Claims of "trust"
  - Hijacked by definition
  - Equated with "availability"
- Cloud auditing … still a work in progress
  - Check ISACA guidance
  - Auditors continue "figuring it out"
- Operational attempts
  - Private/community cloud comfort level
  - Public clouds attempt to use compensating technique of "presumptive security" but need lots of negotiations around SLA, exceptions, penalties, concepts of operation
  - Cloud providers moving to two tier (government and others) delivery, but risk Balkanization of the cloud and cloud business case
  - Case studies

Transparency Restores Information Assurance

Working with a “glass cloud” delivers the elastic benefits of the cloud



As visibility is gained …

- Configurations are known and verified
- Data exposure and use is collected and reported
- Access permissions are discovered and validated
- Processing and data locations are exposed
- Compliance evidence can be gathered and analyzed
- Processing risks and readiness become known

… Security, compliance, and value are captured as well

NASA CTO Recommendations for Government

- “If I may be so bold as to give a few recommendations, I would say **don't wait**. Prototype now, try it now because then you will learn what IT security issues you have and then you can figure out which data you want to put in the cloud and not put in the cloud.”
- “Another recommendation would be to make sure that the **mission is engaged**. This is not an IT win, it's a business win.”
- “**Partner with everyone** who will engage with you, and that's been really good for us, both with the mission side and other IT-type partners, and the vendors themselves. I guess when everything is that new **everybody is learning**, but it has been a very good experience.”
- “And then most of all is to **be visible** and have fun with it, because it has to have potential benefits and it is fun. It is **exciting** to be able to do things **quicker** than you could before and potentially at **much less cost**. The energy creates more energy.”

– Tom Soderstrom, CTO at NASA's JPL

http://www.govinfosecurity.com/articles.php?art_id=3177&rf=2010-12-20

Q&A

Chris Knepper

Partner, Cloud Consulting Practice
CSC

Mike Dorohovich

Army Land Division
CSC